QUANTUM PRIVACY CATALYST NETWORK

Launch Plan & Quantum Privacy Rewards Framework

Version: 7.0 | Date: March 25, 2026

Authored By: Jonathan Hare & Rich Muth

Table of Contents

1. EXECUTIVE SUMMARY 3

2. STRATEGIC OBJECTIVES 9

3. RACE DYNAMICS: ENABLING THE ADOPTION CASCADE 11

3.1 Unified Trust Model Premiums: Principles Governing Trust, Growth & Reward Allocation 11
3.2 Race to the Top (driven by the Strategic and Timing Premiums) 11
3.3 Race to Close (driven by the Value and Cascade Premiums) 12
3.4 Race to Deploy (driven by the Value, Cascade & Governance Premiums) 13
3.5 Race to Leadership (driven by Timing, Publicity & Proportionality Premiums) 14
3.6 The Race to Monetization (driven by the Value, Cascade & Proportionality Premiums) 15
3.7 Race to Empower (driven by Adaptive Compliance, Universal Ownership, Evangelized Mode & MUM) 16
3.8 Game-Theoretic Payoff Structure: Why Immediate Participation Is the Dominant Strategy 19
3.9 Four Independent Adoption Cascades: Why Critical Mass Is Near-Certain 20

4. QUANTUM PRIVACY REWARDS ALLOCATION MODEL 25

4.1 Launch Premiums 26
4.2 Governance Premiums 28
4.3 Adaptive Premiums 32
4.4 Quantum Genomes: How UTM Premiums Are Embedded, Inherited & Amplified 33
4.5 Privacy Network Provider Roles 44
4.6 Ownership, Token Economics & Settlement Mechanics 49
4.7 Exchange Root & Public Benefit Allocation 52
4.8 PNX Settlement Waterfall 53

5. CATALYST CONTRIBUTION CATEGORIES 55

5.1 Classification Logic 55
5.2 The EP3 Contribution Context (Canonical Reference) 55
5.3 Identity & Authentication 56
5.4 Eight Primary Categories 56
5.5 Program Structure: Accelerator → Program → Objectives Hierarchy 57
5.6 The Contribution Type Taxonomy: UX Tier Structure 58

6. COLD-START ARCHITECTURE: OPERATING BEFORE PREREQUISITES EXIST 59

6.1 Inter-QPC Agreements 60
6.2 Migration to On-Ledger Settlement 60
6.3 Person-Centered Aggregation: Bypassing Cross-Enterprise Friction 60
6.4 Layered Encryption: Dual-Key Authorization 62
6.5 Protected Proliferation: Generating Value Before Certification 62
6.6 Deferred Activation Architecture 63
6.7 Jurisdictional Optionality & Entangled Token Embodiment 64
6.8 The QPN as a Meta-Protocol for Coordination and Settlement 65
6.9 Grassroots Cascade: Evangelism, Ownership & Demand 67
6.10 Investment Cascade: Competitive Capital & Ecosystem Acceleration 68
6.11 Sovereign Cascade: From One Government to Global Scale 69

7. IMPLEMENTATION SUMMARY 69

7.1 Six-Layer Architecture 70
7.2 Staged Governance: Delegated → Federated → Cryptographic 71
7.3 Universal Compliance: Safe Deployment without Accreditation 73
7.4 Inside the Trusted Containment: What Can Operate Immediately 88
7.5 Contributor Engagement: The Three-Layer Motivation Model 89
7.6 The QPN Catalyst Application 91

7.7 The Participant Experience and Economic Interface 99
7.8 The Milliman-Anchored Production Environment 104
7.9 Parallel Development Tracks 105
7.10 Core Team Funding Pathways 105
7.11 Implementation Phases 106
7.12 Revenue Timeline 111
7.13 Investment Structure 111

8. USER STORIES: UNIVERSAL OWNERSHIP IN PRACTICE 112

9. CATALYST NETWORKS AND COLLABORATIVE CONTRIBUTIONS 114

9.1 Contribution Visibility Model 117
9.2 Delegated Attribution: Recording Contributions on Behalf of Another Contributor 118
9.2 Connection Strength: The Contributor-Facing Confidence Signal 119
9.3 My Network: Contributor Activity Analytics 119
9.4 Coordination & Opportunity Marketplace 120
9.5 Nearby Opportunities: The Contributor-Facing Objective Feed 120
9.6 The Graph Assembly Problem 121
9.7 AI-Assisted Dispute Resolution 122
9.8 Reward Sharing: Automatic Attribution vs. Negotiated Bounty Terms 122
9.9 The Impact Score 123

10. CATALYST NETWORK SECURITY & PRIVACY ARCHITECTURE 123

10.1 Cryptographic Record Integrity 124
10.2 Zero-Knowledge Foundation 124
10.3 Governed Agent Authorization Boundary 124
10.4 Contributor Sovereignty & Consent 126
10.5 Deferred Activation Mechanics 126
10.6 Audit Trail Architecture & Permanent Privacy Seal 126
10.7 Graph Assembly & Analysis Privacy 128
10.8 Relationship to the QPN/PNX Security & Privacy Architecture 129

APPENDIX A - *FOUNDATIONAL ENABLING SERVICES & CATALYST MODULES* 130

A.1 Introduction & Six-Layer Architecture 130
A.2 Component Summary Table 131
A.4 An Efficient Market for QPN Bootstrapping and Growth 134
A.5 Three-Tier Contributor Model 136
A.6 Vendor Competition for Foundational Network Position 136
A.7 Competitive Frenzy Dynamics: Cascade Trigger Paths 137
A.8 Phase 0: Strategic Rationale in Detail 138
A.9 Attribution Durability: Protocol-Enforced, Not Host-Dependent 139
A.10 Data Rights & Consent: Strategically Amendable, Not Structurally Blocking 139
A.11 Milliman's Incentive Equilibrium: Why the First Hub Wins 140
A.12 FISMA and FedRAMP as Accelerants 141
A.13 Embryonic Network Incubation: Bottom-Up & Top-Down Cascade Mechanisms 142
A.14 From Execution-Sensitive to Execution-Sequenced: No Remaining Gating Factors 144
A.15 Reassessing the Scenario Probability 145
A.16 Cascading Adoption Under the Containment-First Architecture 147

APPENDIX B - *ENGINEERING SPECIFICATIONS* 150

B.1 Patentable Inventions Summary 150
B.3 Catalyst Modules 153
B.4 Three-Stage AI Evaluation Pipeline 164
B.5 Personal Archive, Context Profile & Contributor Intelligence Module 166
B.6 Multi-Substrate Persistence Architecture 168
B.7 Cross-Verification Protocol 170
B.8 Global Contribution Graph Assembly Engine 172
B.9 Settlement Controller 174
B.10 Technical Reference Schemas 176
B.11 Foundational Enabling Services 177
B.12 QPN Catalyst Application & Capture Module Specifications 233

APPENDIX C - *VALUE ACCRUAL FRAMEWORK, UNIVERSAL OWNERSHIP & PARTICIPATION STRATEGY* 259

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

C.0 Purpose & Analytical Framework 259
C.1 The Three-Channel Value Framework ..... Error! Bookmark not defined.
C.2 Ecosystem Value vs. Shareholder Value: How Universal Ownership Transforms Allocation of Returns 267
C.3 Universal Ownership as a Strategic Management Tool 271
C.4 Private Accelerators: The Enterprise Strategic Lever 272
C.5 How Ecosystem Value Translates to Stakeholder Value 273
C.6 The Monetization Uplift Multiple (MUM) & Early-Mover Premium Economics 276
C.7 Long-Run Value Distribution: From Accelerator Concentration to Universal Participation 277

APPENDIX D: THE CONTRIBUTOR-CENTRIC NARRATIVE 280

D-1. The Four Adoption Cascades Are Horizontal and Cross-Propagating 280
D-2. The Dual-Cascade Amplifier 281
D-3. The Premium Multiple: Quantifying Early-Mover Advantage 281
D-4 Accelerator Proliferation and Cross-Amplification 287
D-6 The Fast-Follower Dynamic: Consolation Awards and Incentive-Efficient Evangelism 288
D-7 Total QP Rewards Increase as Premium Multiples Decline 291
D-8 Product Capability Alignment with Accelerator Network Stages 292
D-9 Contribution Integrity, Validation Governance, and Dispute Resolution 296
D-10. Quantified Reward Trajectory by Contribution Type 298
D-11. The Laggard Penalty: Enterprise vs. Individual 300
D-12 Incentive Pool Lock-Down Is Milestone-Driven 301
D-13. Ecosystem-Level Participation Pathways 302
D-14. Immediate Activation: Why the Window Is Now 303

1. Executive Summary

The Quantum Privacy Catalyst Network is the activation platform for the Quantum Privacy Network (QPN) and Privacy Network Exchange (PNX). It creates the contributor ecosystem, rewards infrastructure, and competitive race dynamics that transform a decentralized architecture into a self-funding, self-organizing network effect.

The Catalyst operates as a privacy-preserving "sidecar" system designed to operate alongside standard enterprise workflows — software development, contract execution, AI research, strategic outreach, and advocacy — capturing, classifying, and attributing contributions to QPN, Private and Shared Accelerators, and the PNX ecosystem. It enables the Quantum Privacy Rewards program by creating a verifiable, zero-knowledge audit trail of contributions that can be retrospectively evaluated and rewarded through Exchange Token settlement.

The system addresses the fundamental Dual-Use Dilemma: the most valuable early contributions — code, advocacy, introductions, compliance work — come from professionals currently employed by major enterprises or government agencies who cannot contribute openly without risking employment contracts, IP obligations, or Data Loss Prevention policy violations.

The Core Innovation: Separating Verification from Transfer

The Catalyst resolves the Dual-Use Dilemma by separating the verification of value from the transfer of IP, allowing contributions to be attributed to the individual's Quantum Privacy Cell (QPC) without exposing proprietary content. A Senior Engineer at a Tier-1 Bank can commit Privacy Pipe code, sign the hash with their QPC key, and earn verifiable Quantum Privacy Rewards — without a single line of source code leaving their employer's network.

"If you helped build it, you should own a piece of it." The Deferred Activation architecture makes this promise technically enforceable: contribution records captured today accumulate in the contributor's QPC as cryptographically-signed, tamper-evident attribution claims —

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

independent of any employer, platform, or intermediary — and mature into Exchange Token allocations as the network reaches settlement readiness.

The Quantum Privacy Catalyst Network: A Network of Networks

Every participant in the QPN ecosystem grows their own Catalyst Network — the subgraph of the global contribution graph that they anchor. A **Personal Catalyst Network** encompasses an individual's contributions, the chains those contributions participate in, the people and organizations they've connected, the Resources they've enabled, and the Exchange Networks and Resource Pools they've helped form. An **Enterprise Catalyst Network** is the aggregate graph of contributions made by and through an enterprise — its employees' contributions, its customers' enrollments, its infrastructure's settlement activity, and the Exchange Networks it anchors. Each **Accelerator Catalyst Network** encompasses the contribution graphs of all participants within that Accelerator's programs and objectives. The **Quantum Privacy Catalyst Network** is the interconnected network of all Personal, Enterprise, and Accelerator Catalyst Networks — the global contribution graph from which settlement, attribution, and Quantum Reputation are derived.

Each participant's Catalyst Network is a tangible, growing asset rooted in their Quantum Privacy Cells. It is not a separate system — it is the contribution and reputation layer that sits on top of their Privacy Networks. The Personal Privacy Networks are about rights and governance; the Personal Catalyst Network is about contribution and reputation. Together, they form the complete picture of what a participant owns and what they've built.

Quantum Reputation is a multidimensional, contextual assessment derived from a participant's Catalyst Network and Privacy Networks — a measure of what they have built, who they are, how they conduct themselves, and the value they have generated. Quantum Reputation is earned, not purchased. It accrues along three complementary dimensions:

- **Contribution reputation** reflects what the participant has done: verified contributions with evidence, chain participation leading to outcomes, objective advancement, cross-program breadth, and the downstream settlement value generated by the participant's Catalyst Network.
- **Identity reputation** reflects who the participant is and how trustworthy their attestations are: verified identity credentials, professional qualifications, organizational affiliations, and relationship confirmations — each recorded as Trust Credentials within the participant's QPC. A longer contribution history, more activity across programs and domains, more verified relationships, and more third-party validations and endorsements collectively establish that a participant is real, active, and accountable — making it progressively harder to fabricate a credible Catalyst Network as part of a fraud scheme.
- **Behavioral reputation** reflects how the participant conducts themselves: the ethical quality of their interactions, the fairness of their commercial terms, the accuracy of their endorsements, the impact of their Resources on counterparties and downstream participants, and their track record of honesty, cooperation, and responsible stewardship across the ecosystem.

All three dimensions are multidimensional (not a single score), contextual (per-program, per-Accelerator, per-domain), and portable (they travel with the QPC, independent of any employer, platform, or intermediary).

Quantum Reputation is independently valuable because it makes participants more effective at network formation. A participant with a large, well-evidenced Catalyst Network can serve as a credible channel for making introductions, proposing terms of exchange, contributing

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

resources to Exchange Networks and Resource Pools, and connecting participants and proposals to the right counterparties — through Referrals (which provide access and visibility without staking reputation) and Endorsements (which provide access, visibility, and a reputation-backed attestation of quality). This dynamic embodies a mode of preferential attachment: high-reputation participants attract more connection requests, more collaboration opportunities, and more influence over how Exchange Networks and Resource Pools form. The result is a merit-based flow of capital and attention in which economic advantage accrues to demonstrated contribution, verified identity, and trustworthy behavior rather than to institutional position or capital accumulation.

Privacy Network Provider Roles

Any participant in the Privacy Network Exchange serves as a Privacy Network Provider (PNP) in one or more of five distinct roles: Resource Providers contribute assets and data; Exchange Providers enable Privacy Network infrastructure; Exchange Networks combine and transform Resources into value-added Resource Derivatives; Solution Providers compose Resources into customer-facing products and services; and Engagement Providers drive adoption, enrollment, and ongoing participation. These roles are not mutually exclusive — a single participant can serve in any combination simultaneously — and any role can be delegated to specialized partners. The roles, their economic mechanics, and how they interact through the PNX settlement waterfall are defined in Section 4.4.

Adaptive Compliance and the Authorization Graph

The Quantum Privacy Network's **Universal Compliance** architecture eliminates the regulatory barriers that traditionally prevent cross-organizational data access and reuse. Through Adaptive Compliance, the EasyAccess Authorization Network can dynamically construct privacy-preserving Authorization Graphs that combine the legal, regulatory, and contractual rights of any combination of individuals, enterprises, and governmental entities — assembling compliant access paths to data without bilateral agreements, regulatory exemptions, or data-sharing negotiations. Authorization Credentials are themselves valuable QP Resources published by competing Trust Authorities, creating a competitive marketplace for trust, compliance, and rights enforcement. Individuals hold uniquely powerful rights within this marketplace: their person-centered legal and regulatory rights to data — exercised through Personal Privacy Networks — can eliminate most restrictions on cross-organizational data use, making individual participation the key that unlocks the full economic potential of the network. The architecture described in Section 7.3 details how Adaptive Compliance, Authorization Graphs, and the competitive marketplace for Trust Credentials operate in practice — including how they enable end-to-end personalized services that no single organization could deliver alone.

UTM Premiums and Race Dynamics

The Unified Trust Model (UTM) Premiums guide how contributions are weighted, how rewards are allocated, and how the Privacy Network Exchange matches resources with demand — creating preferential attachment dynamics where participants who embody the network's core principles attract more connections, more reuse, and more settlement value over time.

- **Launch Premiums** (Strategic, Timing, Value, Cascade, and Publicity) create competitive urgency during the bootstrapping phase.
- **Governance Premiums** (Ethics, Reputation, Safety, Freedom, Sharing, Humanity, Nature, and Innovation) embed enduring values into the network's governance DNA — ensuring they persist and compound as the network scales.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Adaptive Premiums** (Proportionality and Balance) dynamically regulate the system to prevent extractive concentration and maintain fairness.

Together, these Premiums drive six interlocking races — **Race to the Top**, **Race to Close**, **Race to Deploy**, and **Race to Leadership** through institutional engagement; the **Race to Monetization** through economics that reward early adoption; and the **Race to Empower** through grassroots empowerment that generates demand from below — each self-reinforcing: winning one race creates structural pressure on participants to enter the others. The race dynamics and mechanisms for enabling them are described in detail in Section 3.

The UTM Premiums are not merely reward-allocation principles — they are structurally embedded in the governance DNA of every QP Resource, Exchange Network, and Resource Pool through what the architecture calls the **Quantum Genome**: a heritable, evaluable governance identity that propagates through every resource reuse, transformation, and recombination event, creating evolutionary selection pressure that progressively aligns the entire ecosystem with the UTM Premiums (Section 4.4).

The adoption dynamics are further reinforced by **four structurally independent adoption cascades — Enterprise**, **Grassroots**, **Investment**, and **Sovereign** — each capable of independently triggering global-scale adoption through distinct mechanisms and distinct participants. All four must independently fail for a critical mass not to be reached. The cascade architecture is described in detail in Section 3.9.

Self-Funding Settlement and the Race to Empower

The UTM Premiums, Privacy Network Provider roles, and Adaptive Compliance architecture described above collectively enable PNX Settlement — whether contractually via the interim dual-use PNX platform or via Quantum Privacy Tokens and Liquidity Pools as they become available — which is the mechanism that makes the Quantum Privacy Network self-funding and freely available to all participants.

The **Monetization Uplift Multiple (MUM)** creates increasing returns to scale: early adopters who establish positions in densely connected Exchange Networks earn disproportionate returns, making early participation the dominant economic strategy. The Race to Empower (Section 3.6) operates through a structurally independent, bottom-up mechanism: individuals are empowered with the tools, rights, and economic incentives to self-organize, form their own Exchange Networks and Resource Pools, lead the transformation to native QPN solutions, and capture a significant share of the wealth created. This generates demand that forces enterprises, capital sources, and governments to adopt quickly and support individual empowerment — creating parallel cascades that reinforce each other across all four adoption pathways — Enterprise, Grassroots, Investment, and Sovereign — all of which must independently fail for critical mass not to be reached.

QPN Catalyst: Signal Input Modes & Capabilities

QPN Catalyst is the application through which participants build and manage their Catalyst Networks. It is the WebVector reference implementation — the general-purpose web application providing contribution capture, portfolio, reputation, and administrative capabilities. “QPN Catalyst” is the product; “WebVector” is its architectural role within the Catalyst Module taxonomy.

The **Catalyst's Contribution Capture** capabilities are organized around **Signal Input Modes**, defined by how contributions enter the system and the level of human intentionality involved:

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Active Capture Mode** captures contributions when a contributor deliberately opens the application (Voice, Paste, Upload, or Manual input).
- **Directed Capture Mode** captures contributions when a contributor sends a signal to the agent within their existing workflow (CC'ing on an email, tagging in Slack, forwarding a meeting summary).
- **Ambient Capture Mode** captures contributions when the agent monitors authorized sources with per-contributor opt-in and detects contribution-worthy activity without explicit human flagging.
- **Institutional Processing Mode** reconstructs contribution history at enterprise scale when an institution authorizes retrospective processing of its data stores (email archives, document repositories, code repositories, CRM records, public filings).
- **Evangelism Mode** generates new contributions through the attribution-tracked distribution of awareness and participation content (EasyAccess Links, vendor portals, social media, influencer content, government announcements), with the evangelizer earning Cascade Premium and Publicity Premium-weighted Quantum Privacy Rewards proportional to the downstream settlement generated by their distribution.

The five modes form a complete contribution lifecycle: Active, Directed, Ambient, and Institutional capture contributions that have occurred; Evangelized generates new contributions that would not otherwise exist. Each mode inherits all governance constraints from the QPC Control Plane.

The Catalyst architecture encompasses the following integrated capabilities:

Catalyst Contribution Capture (Catalyst Modules):

Eight Catalyst Modules — WebVector (general-purpose hub), VoiceVector, CodeVector, DocVector, AgentVector, CommVector, MeetVector, and MessageVector — implemented as lightweight plugins, agents, and a native contributor app that witness and hash work products without extracting content.

- **WebVector** is the general-purpose web application providing multi-modal contribution capture (voice narration, clipboard paste, document upload, structured form entry), contributor portfolio and reputation dashboards, proximity-based objective navigation, contribution graph visualization, administrative program and objective management, and the recording confirmation and receipt workflow. WebVector serves as the primary contributor interface during Phase 0 and the administrative portal for Accelerator Managers across all phases. It is the hub from which specialized Vectors extend — incorporating VoiceVector, DocVector, and CommVector (email intake) capabilities in its initial deployment. The QPN Catalyst application is the first WebVector embodiment;
- **VoiceVector** captures natural-language voice narrations, clipboard-pasted text, and manual form entries through the QPN Catalyst app — the primary contribution interface for Phase 0 and for relationship-intensive contributors whose work does not generate digital artifacts. AI-assisted field extraction processes the narration to produce structured attribution records including contributor identification, contribution type classification, contact and organization matching against the canonical directory, topic extraction, and related-to connection detection. A progressive disclosure recording flow guides the contributor through review, evidence attachment, and a three-step confirmation wizard, completing in under 60 seconds;

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **CodeVector** captures code commits, pull requests, repository contributions, and engineering artifacts through developer toolchain integration (Git hooks, CI/CD pipeline plugins, IDE extensions). Each captured event is hashed at the source without extracting proprietary code, producing an attribution record that verifies the contribution occurred, links it to the contributor's QPC, and preserves chain relationships to upstream and downstream engineering activity. Designed for developers, engineers, and technical contributors whose primary work product is code;
- **DocVector** captures signed agreements, authored documents, governance frameworks, compliance artifacts, and other formal work products through document upload with cryptographic binding. Each uploaded document is hashed (SHA-256) and auto-attached as evidence with rule-based strength classification. Server-side text extraction and LLM-assisted field parsing identify the contribution type, counterparties, and chain relationships. Designed for commercial, legal, governance, and trust-framework contributions that produce formal documentation. Contributors and counterparties can also sign documents directly through their Quantum Privacy Cells using native Privacy Network-enabled signing — free, unlimited, and with stronger cryptographic provenance than commercial e-signature services — eliminating dependence on third-party platforms for formal document attribution;
- **AgentVector** captures AI-assisted research sessions, agentic workflow outputs, and human-AI collaborative work products. Operating primarily in Ambient Mode, the agent monitors authorized AI platforms and tools with per-contributor opt-in, detecting contribution-worthy activity — research findings, analysis outputs, model evaluations, strategy documents — and proposing attribution records for human confirmation. Designed for AI researchers, analysts, and knowledge workers whose contributions emerge through extended AI-assisted workflows rather than discrete events;
- **CommVector** captures outreach, advocacy, and relationship-building activity with verified engagement tracking. In Active Mode, contributors record introductions, meetings, presentations, and advocacy through WebVector. In Directed Mode, contributors CC the Catalyst agent on outreach emails, triggering LLM extraction of structured fields and automatic creation of contribution records with the email as attached evidence. Engagement signals (Meeting Requested, Introduction Requested, Follow-up Sent) capture pre-milestone activity that may later upgrade to confirmed milestones. The SENT → VERIFIED_ENGAGEMENT status progression provides cross-verification of counterparty response;
- **MeetVector** captures virtual meeting transcripts, AI-generated meeting summaries, and in-person meeting notes with end-to-end attribution provenance including speaker identification, topic extraction, action item detection, and chain linkage to prior and subsequent contributions. In Active Mode, contributors paste or upload meeting transcripts through WebVector. In Directed Mode, contributors forward meeting summaries to the Catalyst agent. Native platform integration (Zoom, Teams, Meet webhooks with speaker diarization) is roadmap. Designed for contributors whose primary ecosystem-building activity occurs through meetings and calls;
- **MessageVector** captures inbound messages across email, messaging, fax, and physical mail channels through a privacy-preserving proxy network. Each inbound message is processed by the AI Evaluation Pipeline to determine whether it represents a new contribution, evidence for an existing contribution, a follow-up in an active chain, or routine correspondence. The proxy architecture ensures that message content is never stored in cleartext outside the contributor's QPC-governed Privacy Domain, and that counterparty

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

privacy is preserved through selective field extraction rather than wholesale message retention.

All eight Catalyst Modules feed the same AI Evaluation Pipeline classification stage and produce identical Attribution Records stored in the contributor's local .qpn archive.

AI-Assisted Evaluation:

An intelligent classification layer embedded in the contributor's AI tools (Claude, ChatGPT, Gemini, Grok, Copilot) that semantically evaluates contributions against a canonical **Catalyst Contribution Taxonomy**, generates classification tags and cascade-linkage indicators, and enriches every contribution record with multi-attribute identity anchors for durable entity resolution.

Personal Archive & Contributor Intelligence:

A portable, encrypted, contributor-controlled archive (.qpn file) that stores the contributor's complete attribution history. The Contributor Context Profile (CCP) — a derived document loaded into AI sessions — provides historical context, enables proactive contribution recommendations, auto-populates identity fields for known contacts, and supports cross-session cascade detection.

Multi-Substrate Persistence (Persistence Adapter):

A substrate-agnostic persistence layer that decouples contribution records from any single cloud provider, distributed ledger, or storage system. The Persistence Router writes records across multiple dissimilar substrates (Hedera, cloud databases, local archives, sovereign data stores) with configurable resilience strategies, ensuring durability across decades of technology evolution.

Collaborative Contribution Network:

A controlled-visibility layer enabling contributors to selectively share records with Accelerator Managers and other participants, facilitating cross-verification, coordination matching, capability signaling, and contribution bounties. Visibility is contributor-controlled across four tiers (Private, Manager, Participant, Verified Public) with granular field-level disclosure.

Global Graph Assembly Engine:

An AI-powered service that systematically combines fragmentary contribution graphs from independent, decentralized participants into a unified global contribution graph — linking chain fragments, reconstructing cascade sequences retrospectively, densifying graphs through enterprise dual-use integration, and synthesizing cross-Accelerator attribution.

Settlement & Reward Sharing Module:

An integrated settlement controller that links contribution records to Exchange Token flows, recovers infrastructure costs, and distributes rewards through the QP Reward allocation framework — including automatic graph-based attribution and negotiated bounty-based reward sharing.

The system uses a Sender-Pays / Lazy-Verify computational model: all verification work (hashing, signing, API polling) is performed by the contributor's client-side agent, ensuring zero computational burden on the network until settlement. A Resilience-First persistence strategy ensures contribution records survive device loss, account suspension, and organizational change through encrypted replication across multiple independent substrates.

2. Strategic Objectives

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

The Quantum Privacy Catalyst Network pursues the following interconnected strategic objectives:

- **Dual-Use Enablement:** Allow professionals to earn ecosystem rewards for work performed within private enterprise environments without data leakage.
- **Zero-Knowledge Verification:** Separate the fact of the contribution from the content using cryptographic hashing and opaque-ID tokenization.
- **Frictionless Integration:** Embed seamlessly into existing high-velocity tools (GitHub, VS Code, DocuSign, email clients, AI assistants) via standard APIs and webhooks, with five Signal Input Modes (Active, Directed, Ambient, Institutional, Evangelized) ensuring structurally complete contribution capture across the full contribution lifecycle.
- **Verified Engagement:** Distinguish between mere activity (sending an email) and impact (receiving a reply, closing a deal, deploying a pilot) through cryptographic lineage tracking. SENT upgrades to VERIFIED_ENGAGEMENT only upon confirmed downstream effect.
- **Semantic Classification:** Evaluate contributions against a canonical taxonomy using AI, generating classification tags, cascade indicators, and impact estimates automatically at the point of capture.
- **Durable Entity Resolution:** Enrich every contribution with multi-attribute identity anchors for all referenced persons and organizations, ensuring records remain linkable across job changes, name changes, email loss, corporate mergers, and organizational restructuring.
- **Decentralized Resilience:** Eliminate single points of failure by persisting encrypted contribution records across multiple, dissimilar substrates through a substrate-agnostic Persistence Adapter interface.
- **Contributor Sovereignty:** Maintain contributor control over all contribution records, visibility settings, identity attributes, and disclosure levels — with privacy enforced cryptographically, not by policy.
- **Collaborative Ecosystem Formation:** Enable selective sharing, cross-verification, coordination matching, capability signaling, Referrals, Endorsements, and contribution bounties to accelerate growth of the decentralized contribution graph.
- **Catalyst Network Growth:** Enable every participant — individual, enterprise, and Accelerator — to grow a Personal, Enterprise, or Accelerator Catalyst Network as a tangible, portable asset rooted in their Quantum Privacy Cells, encompassing their contributions, chains, connections, Resources, and Exchange Networks.
- **Quantum Reputation:** Derive a multidimensional, contextual, earned reputation from each participant's Catalyst Network — reflecting both contribution reputation (what they've built) and identity reputation (who they are) — that makes participants more effective at network formation through Referrals and Endorsements, embodies preferential attachment, and creates a merit-based flow of capital and attention.
- **Grassroots Adoption Cascade:** Enable a structurally independent, bottom-up path to critical mass where individuals evangelize the opportunity, accumulate ownership, crowdsource Accelerators, generate demand for QPN-routed products and services, and create competitive forcing functions on incumbents — operating in parallel with and reinforcing the enterprise adoption cascade.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Self-Funding Settlement:** Ensure the system operates as a zero-deficit architecture by processing only claims with sufficient value to cover their own verification and settlement costs.

3. Race Dynamics: Enabling the Adoption Cascade

The objective of the Quantum Privacy Rewards model is to enable the Quantum Privacy Network to self-organize and adapt from initial launch to global ubiquity — aligning incentives so that the network maximizes benefits for its participants and society while remaining safe, efficient, resilient, dynamic, innovative, fair, and healthy.

3.1 Unified Trust Model Premiums: Principles Governing Trust, Growth & Reward Allocation

The **Unified Trust Model (UTM) Premiums** reflect the core principles and values that enable emergent, self-sustaining trust and growth across all participants in the decentralized, self-organizing Quantum Privacy Network. These Premiums guide how contributions are weighted, how rewards are allocated, and how the Privacy Network Exchange matches resources with demand — creating preferential attachment dynamics where participants who embody these principles attract more connections, more reuse, and more settlement value over time. They fall into three categories (defined in detail in Section 4):

- **Launch Premiums** (Strategic, Timing, Value, Cascade, and Publicity) drive allocation during the bootstrapping phase based on who contributed what, when, and how visibly — creating the competitive urgency that triggers cascading adoption while aligning incentives for sustainable growth and equitable value sharing;
- **Governance Premiums** (Ethics, Reputation, Safety, Freedom, Sharing, Humanity, Nature, Innovation) reward contributions that embed trust, safety, equity, sustainability, and human well-being into the network's permanent governance DNA — ensuring that the values shaping the network's formation persist as it scales; and
- **Adaptive Premiums** (Proportionality and Balance) dynamically regulate the system as it grows, ensuring allocation scales with impact, self-corrects over time, and prevents extractive concentration — keeping the network efficient, fair, and responsive to changing conditions at every stage of maturity.

Together, these Premiums create compounding urgency across every dimension of ecosystem formation simultaneously. Six interlocking races drive this dynamic — four operating through institutional engagement, a fifth through monetization dynamics that reward early adoption, and a sixth through grassroots empowerment that generates demand from below — each self-reinforcing: winning one race creates structural pressure on participants to enter the others.

These race dynamics are amplified by four structurally independent adoption cascades — Enterprise, Grassroots, Investment, and Sovereign (Section 3.9) — each capable of independently triggering global-scale adoption, and each reinforcing the others once activated.

3.2 Race to the Top (driven by the Strategic and Timing Premiums)

Senior executive leadership — founders, CEOs, CTOs, board members, managing partners — are uniquely positioned to sponsor and drive enterprise-wide strategic adoption, and, in many cases, to combine strategic commitment with investment and public-benefit commitments.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

The Quantum Privacy Rewards model creates strong incentives for contributors to find a path to direct engagement with this level of leadership as rapidly as possible.

A powerful first-mover dynamic applies: the first individual or team whose contribution graph verifiably reaches senior leadership and triggers a tangible enterprise commitment — a meeting that leads to a strategic partnership, an internal assessment that converts to an Accelerator formation decision — earns significantly more lucrative Quantum Privacy Rewards than contributions that arrive later, after the commitment is already secured.

Multiple, distinct contribution graphs involving different individuals or teams can engage the same enterprise in parallel, each independently working to secure institutional participation and executive engagement. If one graph succeeds first in reaching the C-suite and locking down a strategic commitment, that graph receives a disproportionate share of Quantum Privacy Rewards — while competing graphs receive lesser amounts proportional to the independent adoption they enabled, adjusted by the Proportionality Premium.

Participants in separate contribution graphs targeting the same enterprise can also choose to merge their graphs — coordinating their campaign to reach leadership and drive internal adoption collectively. Merging increases the probability of being part of the first graph to secure a strategic commitment, but distributes the resulting Quantum Privacy Rewards across a broader group. This creates a strategic tradeoff between competition and cooperation: contributors weigh the higher individual reward of winning independently against the higher probability of winning collectively, with the optimal strategy depending on their relative access, progress, and risk tolerance.

The result is constructive competition among contributors targeting the same enterprise — with the option to collaborate when coordination improves collective odds — and the prize going to whoever translates access into commitment fastest.

One major investment or public strategic commitment is sufficient to trigger a competitive commitment cascade. No hyperscaler can let a competitor establish foundational positioning in the privacy exchange layer. No professional services firm can let a rival capture the QPN consulting practice. No financial institution can let a competitor's data assets become the default PNX settlement infrastructure. The architecture is designed so the question is never whether adoption happens — only how fast, and who captures foundational positioning.

3.3 Race to Close (driven by the Value and Cascade Premiums)

The primary objective of the Quantum Privacy Rewards model during the initial launch is to reach Activation Milestones as quickly as possible and scale them as rapidly as possible — through both institutional engagement and grassroots demand formation. Quantum Privacy Rewards are tied to real traction that ultimately contributes to PNX-settled revenue — not to activity for its own sake.

The Catalyst framework distinguishes between three types of milestones:

- **Contribution Milestones**: The actions participants take — introductions, meetings, endorsements, technical validations, advocacy campaigns. These are recorded as Contribution Records in the Catalyst Contribution Ledger.
- **Activation Milestones**: The real-world outcomes those actions produce — enterprise commitments, MOU executions, pilot deployments, public announcements, production settlement. Attribution remains conditional until Activation Milestones verify the chain's effectiveness.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Cascade Milestones**: A high-leverage Activation Milestone that triggers a cascade that drives a transition between ecosystem stages — such as the first Tier 1 Anchor public commitment, which triggers competitive adoption across an entire industry.

Cascade Milestones receive very high Premium Multiples because they produce outsized downstream value and mark structural transitions in the ecosystem's maturation. They are the events that cause the Premium Multiple curve to drop steeply, because the hardest and most validating work has been done.

Early-Stage Contribution Milestones (introductions, endorsements, meetings, proposals, evangelism) serve as the mechanism for allocating Quantum Privacy Rewards among participants in the contribution graph, but they must be verifiably linked to Activation Milestones to earn Quantum Privacy Rewards.

An introduction that never progresses to a partnership agreement, an endorsement that never translates into a pilot, a meeting that never converts to a commitment — these generate attribution that remains conditional — converting to Quantum Privacy Rewards only when subsequent milestones demonstrate that the contribution was part of a chain that produced real activation.

Attribution that cannot be linked to Activation Milestones remains conditional — it may convert later if subsequent events complete the chain, or it may remain unconverted. A submission in isolation is evidence, not an entitlement. The system rewards verified impact, not activity volume.

The same principle applies to grassroots contributions: an EasyAccess Link that drives thousands of PPN enrollments, a social media campaign that triggers crowdsourced Accelerator formation, or an influencer endorsement that shifts consumer demand toward QPN-routed channels — these earn Quantum Privacy Rewards proportional to the downstream settlement their chains generate, while evangelism that produces no measurable enrollment, demand routing, or Exchange Network formation remains conditional. The contribution graph distinguishes between activity that moves the needle and activity that doesn't, ensuring that the Quantum Privacy Rewards framework selects for effectiveness, not effort.

3.4 Race to Deploy (driven by the Value, Cascade & Governance Premiums)

The Foundational Enabling Services create a first-mover competition among technology vendors. For each component, the question is not whether a platform will be integrated into the QPN, but who builds the first integration, when, who accrues the Quantum Privacy Rewards, and how ownership of the resulting Exchange Networks and Resource Pools is allocated.

The most tangible and heavily weighted Institutional Activation Milestones are those that directly drive PNX-settled revenue: Privacy Network–enabling enterprise resources, infrastructure, user populations, vendors, or solutions; signing enterprise customers with specified commercial terms; and establishing strategic partnerships involving revenue sharing, resource commitments, financing, or distribution agreements. These deployment milestones are heavily weighted in Quantum Privacy Rewards allocation for two reasons: they are what ultimately generate Exchange Token settlement flows, and they create reusable, scalable assets — accredited Exchange Networks, populated Resource Pools, proven trust frameworks — that trigger cascading adoption by demonstrating real-world value to subsequent participants.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Because deployed Exchange Networks and Resource Pools inherit the Trust Criteria authored during incubation, the Race to Deploy is also the moment when Governance Premiums become operationally embedded — making deployment decisions among the most consequential acts of governance DNA authorship in the ecosystem.

The vendor's rational calculation: invest $1–3M in engineering for a platform adapter and $50–500K in Proof of Trust certification to secure perpetual settlement revenue from a network targeting trillions in annual volume — or let someone else build it and watch the settlement revenue flow elsewhere. Worse: a third-party adapter optimized for a competing platform could redirect settlement flows away from the vendor entirely.

AI-assisted development (Claude Code, GitHub Copilot, ChatGPT Codex, Gemini Code Assist) reduces per-component development effort by approximately 65% based on early 2026 capabilities — a figure that is likely to improve significantly as AI models and development tools continue to advance rapidly.

Beyond AI tooling, the QPN architecture itself dramatically simplifies solution development, testing, governance, and operations. Universal Compliance eliminates the need to re-engineer compliance for each new deployment. Zero-marginal-cost reuse of existing Resources means components, data, models, and governance frameworks that have already been contributed and governed can be recombined without rebuilding them. Person-centered aggregation through Personal Privacy Networks bypasses the cross-enterprise negotiation that traditionally consumes months of integration effort.

Together, these architectural properties enable fine-grained, recombinant components and Resources to be dynamically composed and distributed at scale — at a fraction of the effort, cost, and risk of traditional approaches. A skilled engineering team can build production-grade adapters for competitor platforms as easily as for their own — turning adapter development from a defensive exercise into a competitive land-grab: the first team to publish a high-quality connector for any given platform captures the Quantum Privacy Rewards for every downstream settlement event that connector enables, regardless of whose platform it targets.

3.5 Race to Leadership (driven by Timing, Publicity & Proportionality Premiums)

Accelerator governance positions — Accelerator Manager roles, Trust Authority seats, EP3 Foundation representation — carry disproportionate influence over contribution graph interpretation, bounty prioritization, premium allocation, and strategic coordination.

Governance Premium allocations reward participants who hold and actively exercise these roles. Leadership positions compound: early Managers shape the contribution taxonomy, calibrate the attribution confidence hierarchy, and set the bounty market norms that all subsequent participants operate within. As participation increases and participants progressively achieve key milestones, the level of Quantum Privacy Rewards for subsequent contributions declines proportionately — creating a race among individuals and contribution graphs to achieve tangible Activation Milestones and secure strategic commitments before the window of maximum reward narrows.

The competitive dynamics are concrete. If contributors driving parallel contribution graphs were advancing simultaneously at Microsoft, Google, Amazon, and Meta — each with internal advocates working to reach senior leadership — and one graph reached the CEO first, resulting in a public commitment to form an Accelerator or actively join an existing EP3 Accelerator, the individuals in that contribution graph would earn a disproportionate share of

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Quantum Privacy Rewards — potentially many billions of dollars more than competing contributors engaging the other enterprises, even if those competing graphs were only days behind. The effect extends immediately across similar prospects: once one hyperscaler commits, the Quantum Privacy Rewards available for securing comparable commitments at peers decline — because the Strategic and Timing Premiums reflect the fact that the first Anchor commitment in a category is the hardest, most validating, and most pivotal, while each subsequent commitment is incrementally easier and less scarce. The competitive defensive adoption dynamics then accelerate the compression further, narrowing the remaining window for maximum Quantum Privacy Rewards at those enterprises.

The threshold for triggering these cascades is remarkably low. Simply signing a publicly referenceable agreement to participate in EP3 Accelerators — in collaboration with the existing 45+ EP3 affiliates that already maintain a critical mass of dual-use data, enterprise customers, and production deployments across Databricks, Azure, AWS, Google Cloud Platform, and Oracle — would be enormously valuable and would likely initiate a competitive cascade among peers. Even more striking: if any major platform were to update its Privacy Statements and Terms of Service and implement the EasyAccess APIs — a technical integration involving hours of engineering work and no incremental capital or operating expenses — it would enable the enrollment of billions of users into Personal Privacy Networks, creating trillions of dollars in ecosystem value from a single, low-cost operational decision. The Quantum Privacy Rewards for the individuals whose contribution graphs enabled such decisions would be proportionally extraordinary.

3.6 The Race to Monetization (driven by the Value, Cascade & Proportionality Premiums)

PNX Settlement — whether contractually via the interim dual-use PNX platform or via Quantum Privacy Tokens and Liquidity Pools as they become available — is the mechanism that makes the Quantum Privacy Network self-funding and freely available to all participants. Settlement converts every contribution, every resource-reuse event, and every privacy-preserving interaction into economic value that flows to the participants who enabled them. This creates the demand that enables efficient markets, funds ongoing growth and development, and kickstarts the Universal Ownership Model — where individuals, enterprises, and institutions earn proportional returns from the networks they help build, rather than paying for access to infrastructure that captures the value they create.

The critical dynamic governing early-mover economics is the Monetization Uplift Multiple (MUM) — the ratio between the settlement value a Resource Provider earns through a high-performance Exchange Network or Resource Pool versus a lower-performance alternative. MUM is not a fixed metric but an emergent property of network topology: it increases as Exchange Networks grow denser, as Resource Pools attract more high-quality resources, as reuse chains deepen across domains, and as AI-mediated optimization improves matching, pricing, and personalization. The result is increasing returns to scale — each additional participant, resource, and reuse event makes the network more valuable for every existing participant, compounding the advantage of early adoption.

Tier 1 Accelerator participants who establish favorable, well-connected positions within the PNX topology — at the nexus of dense networks of value-sharing agreements — and who aggregate high-quality, repeatedly reusable Resource Derivatives, can command premium margins. Not because they extract unfairly, but because their MUM makes it economically rational for Resource Providers to participate even at a lower sharing rate.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Consider: a healthcare data provider earns 5% of $10 billion in settlement through a high-MUM Exchange Network ($500 million), versus 15% of $500 million through a low-MUM alternative ($75 million) — for the same underlying resource contribution. The rational provider chooses the lower percentage with the higher absolute return. This allows early-mover Anchors to sustain premium economics without losing share to competitors offering higher percentage rates. The MUM advantage compounds as early movers accumulate more Resource Derivatives and deeper cross-network reuse relationships — each new connection increases the settlement volume flowing through their position in the topology, which attracts more Resource Providers, which further increases settlement volume, creating a self-reinforcing cycle of growth.

Early adopters who participate in highly connected Exchange Networks and Resource Pools are rewarded with higher margins, faster growth, and more defensible market positions — advantages that translate directly into much higher valuations for their Quantum Privacy Rewards and Exchange Tokens. Because Exchange Token value is linked to the settlement volume flowing through the Exchange Networks and Resource Pools they represent, participants in high-MUM networks hold tokens that appreciate faster and are worth more per unit of settlement than tokens in less connected networks. This creates a powerful incentive to participate early, contribute aggressively, and build connections broadly — because the window for establishing a high-centrality position in the PNX topology narrows as the network matures and the most valuable positions are occupied.

This doesn't create extractive lock-in, because QP Resources are inherently portable, individuals and enterprises can aggregate demand through their own Exchange Networks to gain leverage, and market discipline operates continuously — Exchange Networks that are too greedy lose Resource Providers to competitors offering better absolute returns. The competitive dynamic ensures that MUM advantages flow from genuine value creation — denser networks, better matching, more efficient settlement, superior privacy and compliance — rather than from artificial barriers to exit. Over time, competitive pressure drives an increasing share of settlement value toward Resource Providers and individuals, while Exchange Providers compete on the quality of their networks rather than on the captivity of their participants.

3.7 Race to Empower (driven by Adaptive Compliance, Universal Ownership, Evangelized Mode & MUM)

While the first four races drive ecosystem formation through institutional engagement, the Race to Empower operates through a structurally distinct, bottom-up mechanism: individuals are empowered with the tools, rights, and economic incentives to self-organize, form their own Exchange Networks and Resource Pools, lead the transformation to native QPN solutions, and capture a significant share of the wealth created — generating demand that forces enterprises, capital sources, and governments to adopt quickly and support individual empowerment rather than resist it.

The architecture described in Section 7.3 — Universal and Adaptive Compliance, Authorization Graphs, and the competitive marketplace for Trust Credentials — is what makes this empowerment concrete rather than aspirational. Individuals can exercise their legal and regulatory rights to data through their Personal Privacy Networks, aggregate fragmented records into comprehensive person-centered privacy graphs, and leverage those rights to unlock resources that no single enterprise can access alone. The EasyAccess Authorization Network can construct Authorization Graphs on behalf of individuals that combine enterprise, governmental, and personal Trust Credentials to overcome regulatory barriers to data access

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

and reuse — at zero marginal cost, without bilateral agreements, and without requiring enterprise cooperation. This transforms the individual from a passive data subject into an active economic participant with real bargaining leverage.

The Race to Empower is powered by five independently sufficient motivations that drive individual participation and consumer preference for QPN-routed channels:

- **Economic Empowerment:** Individuals who contribute to Exchange Networks — through data, relationships, referrals, behavior change, or rights assertion — earn Quantum Privacy Rewards and Exchange Token ownership, creating a direct financial stake in the networks they help build. Consumption through those networks is economically rational because it increases the value of their own holdings.
- **Superior Capability:** Personal Privacy Networks powered by Quantum Privacy and Adaptive Compliance offer capabilities that no incumbent platform can match: person-centered data aggregation across all providers and services, AI-powered personalization informed by the full breadth of an individual's data, and privacy-preserving automation that operates across organizational boundaries without exposing sensitive information.
- **Value Alignment:** Networks designed under Universal Ownership allocate more value to individuals than incumbent platforms that extract rent. Every interaction, every data contribution, and every behavioral choice generates settlement value that flows back to the individual rather than being captured by intermediaries.
- **Self-Organization:** Individuals — including employees of enterprises who work in their spare time and in dual-use initiatives — can form their own grassroots Exchange Networks and Resource Pools, define market requirements, crowdsource development, attract funding, and build ownership through investment or in-kind contributions, all without enterprise sponsorship. An employee who recognizes that their employer's data practices are extractive can begin building Privacy Network-enabled alternatives from within, using dual-use deployment on the employer's own infrastructure.
- **Societal Activism and Cultural Engagement:** Contributors who understand the architecture recognize that routing activity through the PNX accelerates the transition to a more equitable economic model — one where individuals are both consumers and owners, and where market forces structurally reduce inequality rather than amplifying it. Beyond economic equity, individuals are empowered to create Exchange Networks, Resource Pools, and Accelerators that directly address issues they care about — keeping children safe online, accelerating cures for diseases, mitigating climate change, protecting the environment, safeguarding personal privacy, or improving educational outcomes. The architecture does not require institutional permission or philanthropic funding to pursue these goals: any individual or group can form a grassroots Accelerator, attract contributors and resources through Quantum Privacy Rewards, and build solutions that generate sustainable PNX-settled revenue proportional to the value they create. Moreover, any cause or topic that gains attention and engagement — sports, music, entertainment, religion, politics, wellness, hobbies, local community organizing — drives PPN adoption, expands the reachable Privacy Graph, and creates valuable Resources that can be reused across Exchange Networks. A fan community that organizes around a sports league, a congregation that builds a faith-based wellness network, or a music community that creates a privacy-preserving artist-to-listener exchange are all building PNX infrastructure and generating settlement value — whether or not they think of themselves as doing so.

The Race to Empower creates a forcing function on incumbents that is independent of and complementary to the enterprise cascade's peer competitive pressure. When a material

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

fraction of an incumbent's user base begins preferring QPN-routed alternatives — not just because the alternative is technologically superior but because users have ownership in it and superior capabilities through it — the incumbent faces a choice that gets worse with every month of delay. Universal Access means individuals can exercise their rights through Personal Privacy Networks that operate on the incumbent's own infrastructure via dual-use deployment, and Adaptive Compliance means Authorization Graphs will emerge that unlock data and resources the incumbent holds without the incumbent's cooperation.

Initially, the incumbent's installed base becomes the substrate for QPN-routed alternatives that layer privacy, ownership, and settlement onto existing systems. Over time, however, these Privacy Network-enabled solutions can evolve to entirely replace the incumbent's infrastructure — messaging services (WhatsApp, iMessage) replaced by Quantum Privacy-native communication networks, electronic health record systems (Epic, Cerner) replaced by person-centered, privacy-protected health networks that are more efficient, offer superior capabilities, and reward their participants rather than subjecting them to extractive data practices and misaligned incentives. The dual-use phase is not the end state — it is the beachhead from which person-centered replacements emerge, built incrementally through crowdsourced development, funded through Quantum Privacy Rewards and Accelerator Incentive Pools, and adopted because participants have ownership in the networks they helped build. The only sustainable strategy for any incumbent is to join the Accelerator Network and participate as a Privacy Network Provider — serving as an Exchange Provider, Resource Provider, Engagement Provider, Solution Provider, or any combination — not merely to preserve revenue during the dual-use phase, but to retain relevance as the infrastructure itself evolves.

Critically, the Race to Empower enables grassroots contributors to crowdsource Accelerators, define market requirements, confirm market demand, attract or crowdsource funding, and accumulate ownership either via investment or in-kind contributions — all without enterprise sponsorship. Employees can lead transformation from within their own organizations, using their personal PPNs to demonstrate value and build grassroots adoption before seeking institutional endorsement. This creates a credible path to critical mass that is independent of the enterprise cascade, meaning the two cascades operate in parallel and reinforce each other. Enterprise adoption becomes a response to demonstrated demand and demonstrated capability rather than a prerequisite for it.

Under the competitive Privacy Network dynamics described in *Quantum Privacy Network: Universal Access, Exchange, Ownership, AI & Abundance* and *Systems & Methods for a Self-Funding, Self-Organizing Quantum Privacy Exchange and Accelerator Network*, individuals can have an unlimited number of Personal Privacy Networks, each anchored by different Exchange Providers competing on commercial terms and **MUM (Monetization Uplift Multiple)**. Whoever drives enrollment can specify the default Exchange Provider and commercial terms. Over the long term, the sustainable competitive advantage is not maximum individual percentage allocation but participation in interconnected Exchange Networks and Resource Pools that generate the highest MUM — because a smaller share of a high-MUM network is worth more than a larger share of an isolated, low-MUM network. This creates structural incentives for enterprises to support grassroots efforts, pool resources to maximize scale, and compete cooperatively within the PNX rather than attempting to resist or circumvent it. Because individuals can freely move their activity across competing PPNs, enterprises face continuous competitive pressure to offer favorable terms to individuals — allocating a greater share of settlement value to Resource Providers, reducing fees, and improving functionality — in order to build loyalty and retain routing preference. This competitive dynamic structurally supports

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

the Universal Ownership model by ensuring that market forces drive an increasing share of economic value toward individuals over time, reducing income and wealth inequality not through redistribution or regulation, but through the natural operation of a market in which individuals are both consumers and owners.

3.8 Game-Theoretic Payoff Structure: Why Immediate Participation Is the Dominant Strategy

The payoff structure for participation is asymmetric, favoring immediate action regardless of what other participants do. For each potential participant, the strategic calculus is: if competitors participate and you don't, you face maximum competitive disadvantage — your market position erodes as settlement flows route through competitors' Exchange Networks, your data assets lose relative value, and your employees and customers earn Quantum Privacy Rewards through competing ecosystems. If competitors don't participate and you do, you capture foundational positioning — first-mover trust taxonomy anchoring, preferential routing, and the full Launch Premium allocation — at negligible cost and risk. If both participate, you share a larger total ecosystem. If neither participates, you forgo the value entirely and leave it to grassroots adoption. In every scenario, participation weakly or strongly dominates non-participation.

Competitive Exclusion Dynamics. The preferential attachment dynamics of the QPN/PNX create winner-take-most effects within each Anchor category. The first AI infrastructure vendor to commit captures trust taxonomy anchoring and routing centrality that compounds with each downstream deployment. The second vendor in the same category faces a structurally smaller opportunity — not because the market is smaller, but because routing relationships, trust inheritance chains, and Resource Derivative lineage have already begun concentrating around the first mover. By the third or fourth entrant, the available incremental opportunity is a fraction of the first mover's. This creates competitive exclusion pressure: within each category, delay is not merely costly — it is progressively more costly, with each passing commitment by a peer making the laggard's eventual participation less valuable.

The Amplification Paradox. As AI systems become more capable and more deeply integrated into business decision-making, AI models trained on PNX-settled data will themselves recommend QPN/PNX participation to enterprises and individuals — because the economic logic is visible in the data they analyze. An AI system evaluating strategic options for a healthcare enterprise will observe that PNX-connected competitors generate more value from the same data assets, achieve higher settlement returns, and attract better talent through Quantum Privacy Rewards. The system's recommendation will be to participate. This creates a self-reinforcing dynamic where AI adoption accelerates QPN/PNX adoption, which generates more data demonstrating the value of participation, which trains future AI systems to recommend participation more strongly — a feedback loop that operates independently of human advocacy or institutional decision-making.

Equal Access and the Universal Ownership Principle

The QPN is built on the principle of Universal Ownership: the opportunity to participate and earn QP Rewards is available to every person and every organization, without gatekeepers, permission requirements, or prerequisites. No account, no employer approval, no institutional sponsorship, and no capital investment is required. This means that no one — regardless of their seniority, authority, or organizational role — has the right to restrict, block, or discourage others from participating on an equal footing. A manager cannot reserve contribution opportunities for themselves by preventing their team from participating. An executive cannot

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

slow-walk institutional adoption to protect their personal positioning in a contribution graph. Any such behavior is counterproductive for everyone involved, including the person attempting it: contribution graphs are richer, more credible, and more valuable when more people contribute to them. An executive whose team is actively building contribution graphs across the organization's ecosystem will earn far more through cascade effects than one who operates alone. Blocking others doesn't expand your share — it shrinks the pie.

Any attempt to monopolize or restrict access is ultimately futile. The Catalyst Network is publicly available and accepts submissions from anyone. Personal-capacity advocacy outside of work cannot be restricted. Contacts, partners, and customers who are excluded from one contribution graph can independently submit through their own channels, creating parallel graphs that compete with — and may overtake — any graph built through restricted access. The architecture is designed so that attempts to centralize control produce worse outcomes for the person attempting it than open, collaborative participation would.

3.9 Four Independent Adoption Cascades: Why Critical Mass Is Near-Certain

The QPN/PNX architecture does not depend on a single adoption pathway. Four structurally independent cascades can each independently trigger global-scale adoption — and each reinforces the others once activated. Critical mass does not require all four to fire simultaneously; it requires only that one fires with sufficient momentum to trigger competitive responses across the other three. The probability that none of the four fires approaches zero as awareness spreads, because each cascade operates through distinct mechanisms, distinct participants, and distinct incentive structures.

Enterprise Cascade

The Enterprise Cascade operates through two reinforcing mechanisms: competitive pressure and ecosystem activation. When one enterprise in a sector commits as a Tier 1 Accelerator anchor, its competitors face immediate competitive exclusion risk — the first mover captures routing centrality, trust taxonomy anchoring, and Incentive Pool allocations that late entrants cannot replicate. But equally important, the anchor's commitment creates low-friction, dual-use adoption pathways across its entire ecosystem that did not previously exist. With explicit enterprise sponsorship, customers, suppliers, vendors, and governmental counterparties can now participate through existing business relationships, using existing infrastructure, under existing compliance controls — dramatically reducing the friction that would otherwise slow both grassroots and enterprise adoption across the anchor's network. A pharmaceutical company's Accelerator participation does not merely create competitive pressure on peer pharma companies — it creates immediate, sponsored on-ramps for its CRO partners, its cloud providers, its auditors, its hospital system customers, and the patients and clinicians within those systems. Each new participant increases the settlement density that makes participation more valuable for every other participant, creating self-reinforcing adoption dynamics within and across sectors.

The Enterprise Cascade can be triggered by a single enterprise commitment — a hyperscaler founder investing, a Big 4 firm launching a QPN practice area, a healthcare system deploying the Lokahi model, or a financial institution launching a Financial Services Accelerator. The embryonic network incubation pattern means that a single relationship owner within any of these organizations can create a functional micro-ecosystem inside trusted containment, using existing infrastructure, under existing compliance controls, at zero incremental cost. Once the first instance demonstrates settlement value, replication cost collapses and growth

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

becomes exponential — not only through competitive imitation but through the ecosystem pathways that the anchor's commitment has already opened.

Grassroots Cascade

The Grassroots Cascade operates through individual empowerment — the Race to Empower (Section 3.7) in which individuals are equipped with the tools, rights, and economic incentives to self-organize, form their own Exchange Networks and Resource Pools, and drive adoption from below. Through Evangelized Mode, individuals earn Quantum Privacy Rewards for attribution-tracked distribution of awareness and participation content. Through Personal Privacy Networks, individuals exercise person-centered legal and regulatory rights to data that no enterprise can access without their authorization. Through Adaptive Compliance and Authorization Graphs, individuals can dynamically construct compliant access paths to their own data across organizational boundaries.

The Grassroots Cascade creates demand-side forcing functions on enterprises — consumer preference for QPN-routed channels through financial incentive, value alignment, and societal activism — that are complementary to but independent of the Enterprise Cascade's peer competitive pressure. The grassroots mechanism maps directly onto the affiliate marketing, influencer, and creator economy infrastructure that already drives global consumer adoption at scale. Billions of people already participate in referral programs, affiliate networks, and influencer-driven product discovery — the QPN's Evangelized Mode offers the same low-friction mechanics but with ownership rather than one-time commissions. LabLab.ai's community of 250,000+ AI builders, already engaged through the inaugural Lokahi Healthcare Accelerator Hackathon, demonstrates the operational viability of this pathway.

Investment Cascade

The Investment Cascade operates through the same competitive dynamics currently driving hundreds of billions of dollars in annual AI infrastructure investment — but with fundamentally superior capital efficiency. A single credible investor backing the QPN with sufficient funding to independently develop the Quantum Privacy Catalyst Network and Foundational Enabling Services would anchor a Quantum Privacy Investment Network, providing funding through EP3 Networks and various Accelerators — and would trigger competitive investment responses from peer investors who cannot afford to let a rival establish foundational positioning in the privacy exchange layer.

The parallel to the current AI investment cascade is direct and instructive. AI investors are pouring hundreds of billions of dollars into ecosystem infrastructure at stratospheric valuations, teaming with hyperscalers, AI labs, and enterprise customers to build out compute, models, and applications. The QPN investment thesis is structurally superior: the computing infrastructure is dual-use (the same infrastructure already being deployed for AI), the incremental cost is a fraction of AI infrastructure investment, settlement revenue begins from day one rather than requiring years of infrastructure build-out, and the addressable value is GDP-scale rather than sector-specific. An investor who recognized the AI infrastructure opportunity early and deployed capital aggressively captured extraordinary returns; the QPN investment opportunity is analogous but operates at a larger scale with lower capital requirements and faster settlement economics.

A single anchor investor commitment — whether from a technology founder, a venture or growth equity firm, a sovereign wealth fund, or a corporate venture arm — would de-risk the opportunity for subsequent investors, triggering the same competitive investment frenzy that drives AI infrastructure spending. The QPN requires hundreds of millions per major participant, not tens of billions — meaning the capital efficiency of the Investment Cascade is orders of

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

magnitude higher than the AI infrastructure investment cycle it parallels. The Quantum Privacy Investment Network provides the coordinating mechanism: investors participate through Accelerator investments via conventional instruments (SAFE Notes, convertible notes, equity), receiving Accelerator Token allocations from the 20% Incentive & Investment Pool, with Quantum Privacy LLC Managers exercising a right of first refusal to ensure alignment and prevent extractive capital structures.

Sovereign Cascade

The Sovereign Cascade operates through government-driven adoption — a single sovereign entity anchoring a Sovereign Accelerator to develop the infrastructure and services that any government needs to serve its constituents: healthcare delivery, education, workforce development, public safety, environmental monitoring, citizen services, identity management, and regulatory enforcement. The QPN's architecture is uniquely aligned with sovereign priorities because it preserves governmental authority, enhances regulatory enforcement capabilities, and creates economic value that flows to citizens rather than being extracted by platform intermediaries.

A single sovereign commitment would trigger adoption through three reinforcing mechanisms. First, direct funding — whether through government grants, procurement contracts, or sovereign wealth investments — provides the capital to develop domain-specific Exchange Networks and Resource Pools tailored to public-sector needs. Second, government adoption de-risks the opportunity for enterprises, investors, and other sovereigns, because a government anchor provides the regulatory credibility and institutional legitimacy that private-sector participants require before committing at scale. Third, the capabilities developed for one sovereign proliferate to other sovereigns through shared vendors — the Big 4 professional services firms, hyperscalers, systems integrators, and specialized government technology providers that serve multiple governments simultaneously. When PwC deploys a QPN-enabled citizen services platform for the State of Hawaii, the same capabilities become immediately available to every other government client PwC serves — creating cross-sovereign cascade dynamics that operate through existing vendor relationships rather than requiring direct government-to-government coordination.

The State of Hawaii's statewide health transformation initiative — already funded and anchoring the Lokahi Healthcare Accelerator — demonstrates the viability of this pathway. Hawaii's initiative provides the proof-of-concept that other sovereigns can evaluate: a production deployment on existing infrastructure, in a regulated domain, with funded institutional commitment. As the Lokahi model demonstrates settlement value in healthcare delivery, education, and public services, other states, national governments, and international organizations face the same competitive dynamics that drive enterprise adoption — the first sovereign to commit captures governance anchoring and trust taxonomy positioning that later entrants cannot replicate.

Cascade Independence and Mutual Reinforcement

The four cascades are structurally independent — each can reach critical mass without the others. An Investment Cascade can fund development and deployment independently of enterprise commitments. A Sovereign Cascade can anchor institutional adoption independently of private-sector participation. A Grassroots Cascade can generate demand-side forcing functions independently of enterprise or government action. An Enterprise Cascade can propagate through competitive dynamics independently of external funding or government endorsement.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

But they are also mutually reinforcing. An Investment Cascade accelerates the Enterprise Cascade by funding Accelerator formation and reducing participation risk. A Sovereign Cascade accelerates both the Enterprise and Investment Cascades by providing regulatory credibility and institutional proof-of-concept. A Grassroots Cascade accelerates the Enterprise Cascade by creating demand that forces enterprises to respond. An Enterprise Cascade accelerates the Investment Cascade by demonstrating settlement value that justifies further capital deployment.

All four cascades must independently fail for critical mass not to be reached. Given that each operates through distinct mechanisms, distinct participants, and distinct incentive structures — and given that a single trigger event within any cascade can initiate the chain reaction — the compound probability of non-cascade is vanishingly small once awareness reaches a sufficient threshold. The gating constraint is not technology, capital, regulation, or any specific partnership. It is awareness and understanding.

Why Global Cascading Adoption Is More Likely Than Not

The four independent adoption cascades described above establish that critical mass is structurally near-certain — but a reasonable reader may still question whether theory translates to practice. The strongest evidence that it does is not the cascade architecture itself but the fact that the QPN has been explicitly designed to eliminate or structurally mitigate every major barrier that has historically prevented decentralized, multi-stakeholder systems from reaching critical mass.

The Quantum Privacy Network, the Quantum Privacy Catalyst Network, and the Quantum Privacy Accelerator Network collectively address these barriers:

- **Cold-start problems** are eliminated by **dual-use deployment on existing infrastructure**;
- **Regulatory friction** is eliminated by **Universal Compliance** and **Adaptive Compliance**;
- **Coordination costs** are eliminated by **incentive alignment through UTM Premiums**;
- **Capital requirements** are eliminated by **crowdsourced development** funded through Quantum Privacy Rewards;
- **Enterprise resistance** is bypassed by **individual rights-driven adoption** through Personal Privacy Networks;
- **Competitive lock-in** is prevented by **Universal Access** and **resource portability**;
- **Trust deficits** are resolved by **Proof of Trust** and **Quantum Reputation**; and
- **Incentive misalignment** is corrected by **Universal Ownership**, which ensures that every participant earns proportional returns from the networks they help build.

When every structural barrier has a designed-in mitigation mechanism, the question shifts from "can this scale?" to "what would prevent it from scaling?" — and the answer requires identifying a specific architectural failure, not a generic adoption heuristic.

Seven specific facts reinforce this assessment:

- **First, the technology industry is already investing at precisely the scale necessary to drive global adoption.** Hundreds of billions annually in AI infrastructure — data centers, chips, power, and models — with far longer payback periods and far less certain returns than the QPN's infrastructure-light, settlement-from-day-one model. More importantly, the computing infrastructure being deployed for AI development and operation is inherently dual-use — the same data centers, cloud platforms, AI models, and analytics pipelines will naturally be assimilated into the QPN ecosystem as Foundational Enabling Services at zero

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

incremental cost, because the QPN layers trust, governance, and settlement onto existing infrastructure rather than requiring new build-out.

- **Second, the competitive dynamics that drive AI infrastructure spending apply identically to the QPN — but with stronger strategic urgency.** No hyperscaler can let a competitor establish a foundational position in the privacy exchange layer. The QPN directly addresses the economic, trust, safety, governance, and alignment challenges that currently limit AI's commercial and societal potential (as described in Section 4 of *Quantum Privacy Network: Universal Exchange, Ownership & AI*), meaning the strategic value of an early position extends well beyond privacy infrastructure into the core economics of the AI industry itself. This gives AI infrastructure investors a strong incentive to join early and allocate a portion of their existing investments to lead QPN adoption rather than waiting for others to establish the foundational position. The difference in capital requirements makes this even more compelling: where AI infrastructure requires tens of billions per hyperscaler and years to deploy, the QPN requires hundreds of millions per major participant and months to begin generating settlement revenue.
- **Third, adoption does not require any organization to make a top-down decision before value begins flowing.** The embryonic network incubation pattern means a single relationship owner — a partner, an account executive, a program director — can create a functional micro-ecosystem within an existing client engagement, inside trusted containment, using existing infrastructure, under existing compliance controls, at zero incremental cost. Once the first instance exists, replication cost collapses, and growth becomes exponential.
- **Fourth, four structurally independent adoption cascades operate in parallel.** Even if the enterprise cascade proceeds more slowly than projected, three additional cascades can independently trigger critical mass: individuals evangelizing the opportunity through Evangelized Mode, accumulating ownership through Active and Directed contributions, and crowdsourcing Accelerator formation (Grassroots Cascade); a single credible anchor investor funding development and Accelerator formation through the Quantum Privacy Investment Network (Investment Cascade); or a single sovereign entity anchoring a Sovereign Accelerator that provides institutional credibility and proliferates capabilities through shared vendors (Sovereign Cascade). Each cascade operates through distinct mechanisms, distinct participants, and distinct incentive structures. The grassroots cascade creates demand-side forcing functions on incumbents — consumer preference for QPN-routed channels through financial incentive, value alignment, and societal activism. The investment cascade parallels the competitive dynamics currently driving hundreds of billions in AI infrastructure spending, but with superior capital efficiency. The sovereign cascade provides the regulatory credibility and institutional legitimacy that de-risks the opportunity for all other participants. All four cascades must independently fail for critical mass not to be reached.
- **Fifth, grassroots adoption fits naturally into the existing consumer online ecosystem.** The combination of EasyAccess Links, attribution-tracked distribution, and settlement-linked rewards for evangelism maps directly onto the affiliate marketing, influencer, and creator economy infrastructure that already drives global consumer adoption at scale. Billions of people already participate in referral programs, affiliate networks, and influencer-driven product discovery — the QPN's Evangelized Mode offers the same low-friction mechanics but with ownership rather than one-time commissions. This is not a new behavior requiring consumer education; it is a superior version of an existing behavior that the consumer internet has already trained billions of people to perform. The multi-sided

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

network business model of the consumer online world — where platforms, creators, advertisers, and consumers interact through shared economic incentives — is structurally aligned with the QPN's Universal Ownership model, except that under Universal Ownership, the value flows to participants rather than being extracted by platform intermediaries.

- **Sixth, the foundational infrastructure and ecosystem engagement are not hypothetical.** Milliman's production infrastructure already operates at a global scale, supporting thousands of enterprise and governmental clients on Databricks, Azure, AWS, and Google Cloud Platform. Eight EP3 Accelerators have been formed, and launch agreements with over 45 EP3 affiliate organizations have been signed — including global players such as ICON Plc. The State of Hawaii's statewide health transformation initiative that anchors the Lokahi Healthcare Accelerator is already funded. Hedera has already funded WebShield and EP3, the initial technical integration has been validated, and Hedera's Governing Council includes Google, IBM, Dell, ServiceNow, Wipro, Tata Communications, Deutsche Telekom, FedEx, Nomura, Standard Bank, and other Global 1000 enterprises. LabLab.ai has managed the inaugural Lokahi Healthcare Accelerator Hackathon, laying the foundation for grassroots development of Foundational Enabling Services and Catalyst Modules via their global community of over 250,000 AI builders and relationships with leading AI vendors. This is not a whitepaper describing a future system — it is an operational ecosystem with production infrastructure, signed agreements, funded initiatives, and active participants across multiple domains.
- **Seventh, the architecture is designed to make participation the dominant strategy regardless of whether one believes in the system's ultimate success.** Under asymmetric optionality — where participation cost is negligible, early allocation is durable, upside is convex, downside is bounded, and support can be confidential — rational actors participate both opportunistically and defensively rather than waiting for proof of monetization. The game-theoretic payoff structure (Section 3.8) demonstrates that immediate participation dominates delay under every plausible scenario. This means adoption does not require consensus, conviction, or coordination — it requires only that participants recognize that the cost of being wrong about participating is negligible, while the cost of being wrong about not participating is potentially enormous.

For most potential participants — whether senior executives, founders, investors, government officials, developers, clinicians, or individual contributors — this is not a difficult decision. They simply need to know the opportunity exists, that it is in play, and that others in their competitive or professional landscape may already be moving. That is exactly the function the Quantum Privacy Rewards framework and the Race to Empower are designed to serve.

4. Quantum Privacy Rewards Allocation Model

Each Accelerator’s governance framework defines its own Quantum Privacy Rewards allocation model for a designated share of its Incentive & Investment Pool, tailored to its specific context, strategic priorities, and stage of development. There is no single fixed allocation formula: different Accelerators may adopt different, adaptive models reflecting their domain, participant mix, competitive dynamics, and maturation stage.

While specific formulas vary by Accelerator, the Unified Trust Model (UTM) Premiums that govern how Quantum Privacy Rewards are weighted fall into three categories: **Launch Premiums**, which drive allocation during the bootstrapping and incubation phase; **Governance Premiums**, which reflect dimensions structurally embedded in the QPN/PNX

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

architecture that operate continuously once Exchange Networks and Resource Pools are live; and **Adaptive Premiums**, which govern the dynamic regulation and self-correction of the system as it grows.

All allocation determinations are governed by the QP Rewards Allocation Model, a systematic framework guided by the Unified Trust Model Premiums — including the Strategic, Timing, Value, Cascade, and Publicity Premiums — that evaluates contributions based on verified causal linkage, relative timing, independent corroboration, and downstream impact, as assessed by Quantum Rating Schemes and the applicable premium framework. The Managers of Quantum Privacy LLC retain sole and absolute discretion over the design, calibration, and interpretation of the Allocation Model, but individual allocations are determined by the model's application to the contribution graph, not by ad hoc managerial decisions. No explicit reward-sharing agreement is needed for standard graph attribution.

Managers can impact allocation outcomes through specific governance-level mechanisms that serve as inputs to the Allocation Model: verifying contributions that cannot be independently verified through automated means (such as confirming that a meeting occurred or that an introduction led to a specific outcome); specifying strategic targets or bounties for specific objectives within Accelerator Programs; and verifying completion of MOUs, contracts, or strategic partnerships that involve EP3 Accelerators or Quantum Privacy LLC Managers.

These are governance-level inputs to the model — calibrating and enriching the data the model operates on — not overrides of the model's outputs. The distinction is important: the model determines allocations systematically based on verified evidence; the Managers ensure the evidence is as complete and accurate as possible.

During Phase 0, the QPN Catalyst application's behavioral activation system (10 contributor levels, 24 badges, dual XP streams, evidence bonuses, and streak multipliers) provides the real-time visible signal that contributions are being recorded and valued while the Quantum Privacy Rewards settlement infrastructure matures. See Section 7.5 for Phase 0 engagement mechanics and Section 7.6 for the deployed Catalyst application architecture.

4.1 Launch Premiums

Launch Premiums govern Quantum Privacy Rewards allocation based on *who did what, when, and how visibly* to get the ecosystem off the ground:

- **Strategic Premium:** Securing an Anchor entity's public, contractual commitment is the single most valuable early event in the Accelerator Network — because it validates the model, compresses risk perception for every subsequent participant, triggers competitive defensive adoption dynamics, and opens low-friction adoption paths across the entity's entire ecosystem of customers, vendors, partners, employees, and online user populations. Contributions causally linked to securing an Anchor commitment earn Quantum Privacy Rewards reflecting the outsized, non-replicable leverage of that contribution. A verified introduction to a senior executive or founder at one of the largest AI vendors, if traced through the contribution graph to an enterprise-wide strategic Accelerator commitment, could easily be worth billions of dollars for Tier 1 Accelerators.
- **Timing Premium:** Earlier contributions are more valuable than later ones — not merely because they came first, but because they are scarcer, harder, and more pivotal. The first Anchor commitment is harder to secure than the fifth; the first sponsored pilot is harder to secure than the tenth. As adoption progresses and the value proposition is validated by real-world results, each incremental contribution becomes less scarce and less pivotal. The Quantum Privacy Rewards framework reflects this natural scarcity gradient:

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

contributions that occur earlier in the adoption cycle and convert into tangible commitments faster earn proportionally larger Quantum Privacy Rewards. The window for maximum Quantum Privacy Rewards is now.

- **Value Premium:** In the early stages, Accelerator Managers, EP3 leadership, or AI agents deployed by Accelerators can identify high-priority strategic targets — specific individuals, organizations, resource categories, or regulatory jurisdictions — whose participation would disproportionately accelerate network formation, settlement density, or cross-domain reuse. Contributions that successfully activate these high-priority targets earn enhanced Quantum Privacy Rewards reflecting the strategic value of the specific outcome achieved. As the PNX ecosystem matures and the Quantum Rating Scheme develops trustworthy, objective value metrics anchored in the Trust Taxonomies embedded across Exchange Networks and Resource Pools, Value Premiums progressively shift from leadership-designated priorities to evidence-based, algorithmically derived valuations — with Deferred Activation ensuring that retrospective value measurements can be reflected in Quantum Privacy Rewards allocations as outcomes are verified over time.
- **Cascade Premium:** Contributions that generate downstream activation — where one participant's engagement triggers participation by their customers, vendors, partners, or personal and professional networks — earn Quantum Privacy Rewards not only for the initial contribution but for the verified cascade it produces. This reflects the compounding nature of network formation: an introduction that leads to one Anchor commitment, which triggers ten enterprise adoptions, which activate thousands of individual participants, creates exponentially more value than a contribution that terminates at a single node. The contribution graph traces these cascading effects back to their various origins, rewarding the individuals who initiated or amplified chain reactions proportionally to the total settlement generated by those chains.
- **Publicity Premium:** Contributions that are made publicly, promoted openly, or conducted through collaborative structures — such as participation in Shared Accelerators, cross-organizational projects, open standards development, and public endorsements of the QPN/PNX — earn higher Quantum Privacy Rewards than equivalent contributions made privately, under NDA, or restricted to purely proprietary approaches. Public commitments compress risk perception across the entire ecosystem, signal credibility to undecided participants, and generate organic awareness that accelerates adoption at no marginal cost. This applies equally to enterprises and individuals: an executive who publicly champions their enterprise's Accelerator commitment creates more downstream activation than one who participates quietly; a technical team that contributes reusable components through a Shared Accelerator generates more cross-network value than one that develops equivalent capabilities behind closed doors. High-profile individuals, recognized domain experts, prominent investors, and cultural influencers with large public followings can earn premium Quantum Privacy Rewards for public advocacy and outreach, because their endorsement shifts belief alignment among audiences whose participation matters most — accelerating Personal Privacy Network enrollment and broadening the demand-side foundation of the ecosystem. Viral content, educational campaigns, and grassroots advocacy that drive measurable adoption — PPN enrollments, Accelerator formation, Exchange Network growth, or new product and service initiatives that generate PNX settlement — earn Publicity Premium weighted Quantum Privacy Rewards proportional to the downstream activation they produce, creating a structurally self-funding distribution engine where effective evangelism compounds into durable economic participation.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

4.2 Governance Premiums

Launch Premiums govern Quantum Privacy Rewards allocation during the Accelerator incubation phase — but the principles that shape early allocation do not end when an Accelerator's Exchange Networks and Resource Pools reach operational maturity. They become embedded as Trust Criteria and governance policies within the Trust Blocks of every Resource Derivative the Accelerator produces — functioning as governance DNA that shapes the emergent behavior of Exchange Networks and Resource Pools long after they leave the incubator.

Governance Premiums are the dimensions along which this DNA varies. They operate continuously and automatically through the common architectural services — shaping resource matching, utilization probability, trust-weight accumulation, Quantum Reputation, and Exchange Token flows — rather than through discretionary allocation decisions.

Because every generation of Resource Derivatives inherits the Trust Criteria and Trust Credentials embedded in upstream Trust Blocks, Governance Premiums propagate through the ecosystem like genetic traits: resources aligned with high-ethics, high-reputation, high-safety Trust Criteria are preferentially matched, more frequently utilized, and generate stronger Exchange Token streams, while resources burdened with predatory, non-cooperative, or unsafe Trust Criteria are progressively excluded through Proof-of-Trust-driven evolutionary selection pressure — functioning as a built-in immune system that eliminates harmful resources from contributing to future derivatives.

Collectively, the Governance Premiums constitute a multi-dimensional objective function that guides not only resource allocation and Exchange Token economics but the growth trajectory and ownership distribution of the QPN itself — ensuring that the system evolves toward the values encoded in its founding governance DNA rather than toward the interests of any centralized authority. The choices made during the Accelerator incubation phase — deciding which Premium principles are emphasized, how Trust Criteria are authored, what governance policies are embedded in founding Resource Derivatives — have compounding, multi-generational effects on the character of the ecosystem that those Accelerators produce. Early Accelerators are not merely bootstrapping mechanisms; they are authoring the governance genome of the PNX-settled economy.

Governance Premiums reflect the following dimensions, each structurally embedded in the QPN/PNX and continuously shaping resource utilization, Exchange Token generation, and long-run Quantum Privacy Rewards value:

- **Ethics Premium:** Truthfulness, fairness, and responsibility — operationalized through the QPN's Reciprocal Fairness Doctrine, Proof-of-Trust verification, and inherited Trust Criteria. Participants who misrepresent the quality, characteristics, or provenance of their contributions — or who specify commercial terms that disproportionately benefit themselves without regard to the impact on counterparties or broader populations — earn reduced Quantum Privacy Rewards, and their resources face diminished utilization across Exchange Networks. Because ethical dimensions are often difficult to assess objectively at the time contributions are made, the Deferred Activation Model enables retrospective incorporation of outcome data, counterparty performance, fairness metrics, and impact assessments — creating a system that progressively reduces participants' ability to benefit from deceptive or extractive behavior and in which the most ethical participants are also the most economically rewarded.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Reputation Premium:** Quantum Reputation within the QPN/PNX is multidimensional — spanning ethics, performance, compliance, interoperability, privacy protection, trust, safety, innovation, and domain expertise — and contextual: the same participant may express different reputation profiles depending on the usage scenario, jurisdiction, counterparty, Trust Authority, Trust Taxonomy, or Resource Pool in question.

  Quantum Reputation accrues along three complementary dimensions: **contribution reputation** (what the participant has built — verified contributions, chain participation, objective advancement, downstream settlement value), **identity reputation** (who the participant is — verified credentials, organizational affiliations, and a history of trustworthy attestations recorded as Trust Credentials), and **behavioral reputation** (how the participant conducts themselves — the ethical quality of their interactions, the fairness of their commercial terms, the accuracy of their endorsements, the impact of their Resources on counterparties and downstream participants, and their track record of honesty, cooperation, and responsible stewardship across the ecosystem).

  All three dimensions are derived from objective assessment of behaviors and outcomes over time and from attestations and certifications issued by independent Trust Authorities or other participants, all computed within Privacy Domains without revealing personally identifiable information.

  Higher-reputation participants attract more favorable commercial terms, greater resource utilization, and more effective network formation through Referrals and Endorsements — directly driving stronger Exchange Token flows and more valuable Quantum Privacy Rewards. The accountability mechanism ensures integrity: participants who use their Quantum Reputation to endorse proposals, validate other participants, or attest to Resource quality stake their reputation on those endorsements, with failed attestations negatively affecting their Quantum Reputation — particularly their behavioral reputation, which reflects the reliability and honesty of their attestations over time.

  To prevent reputation from becoming a barrier to entry, the architecture provides mitigation pathways for new participants — including supplemental accreditations, performance guarantees, and adaptive governance mechanisms — ensuring that Quantum Reputation functions as a competitive advantage earned through contribution, verified identity, and trustworthy behavior, not a structural barrier that reinforces incumbency.

- **Safety Premium:** Safety encompasses the full spectrum of harm prevention — AI safety and alignment, human physical and psychological safety, cybersecurity, privacy protection, environmental and ecological integrity, financial risk management, public health, and systemic resilience.

  Contributions that improve safety outcomes earn enhanced Quantum Privacy Rewards at both the individual level (security hardening, privacy enhancement, adversarial testing) and the population level (reducing addiction, preventing data breaches, improving clinical safety, strengthening AI alignment).

  Resources that undermine safety metrics face graduated enforcement: economic penalties through reduced trust-weights and compressed Exchange Token generation for moderate risks, and escalating to mandatory audit requirements, resource throttling, surcharges, or full Proof-of-Trust credential revocation for serious risks — particularly those imposing harm on third parties who are not parties to the transaction and receive no compensating benefit.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Safety is not an external constraint; it is an emergent economic property of a system in which the most beneficial behavior is also the most profitable.

- **Freedom Premium:** Resources, Exchange Networks, Resource Pools, and Engagement Networks governed by Trust Criteria aligned with foundational freedoms — ***freedom of speech, freedom of association, freedom of commerce, freedom of choice, freedom of conscience, and freedom from surveillance*** — earn premium Quantum Privacy Rewards, preferential matching, and more favorable commercial terms.

  The QPN/PNX architecture treats these freedoms not as aspirational values but as foundational **constitutional guardrails** of the Unified Trust Model. Privacy-preserving design — the structural expression of freedom from surveillance — is inherent in the architecture: all interactions flow through Quantum Privacy Cells and Privacy Domains where computation occurs without exposing personally identifiable information, ensuring that freedom from surveillance is an engineering property of the system, not a policy preference.

  Critically, privacy preservation does not mean anonymity without accountability. The Quantum Privacy Network enables information to be linked and analyzed globally — detecting risks, evaluating performance, enforcing compliance, and identifying patterns of abuse or criminal behavior — without revealing sensitive or identifiable information to any person, organization, or system. Bad behavior — extractive commercial terms, unreliable endorsements, fraudulent attestations, harmful Resource contributions, or consistently abusive interactions — privately degrades a participant's Quantum Reputation (particularly its behavioral dimension), progressively restricting their economic opportunities, influence over network formation, ability to make credible Endorsements, and access to high-MUM Exchange Networks and Resource Pools. The participant experiences the consequences of their behavior without their identity or specific conduct being exposed to other participants — accountability through economic effect rather than public disclosure.

- **Sharing Premium:** Resources, Exchange Networks, and Resource Pools governed by Trust Criteria that broadly and openly share value with other participants across the PNX — through interoperable resource access, equitable commercial terms, cross-network reuse permissions, and open contribution to shared infrastructure — earn premium Quantum Privacy Rewards, preferential matching, and stronger Exchange Token flows relative to equivalent resources governed by closed, proprietary, or exclusionary Trust Criteria.

  The Sharing Premium is the economic expression of the Universal Ownership model: it ensures that the governance DNA embedded in Trust Blocks structurally favors openness, broad participation, and equitable distribution of value over concentration, extraction, and lock-in. Resources contributed through Shared Accelerators, open standards initiatives, and cross-organizational Resource Pools generate higher reuse density and broader Exchange Token settlement than equivalent resources restricted to proprietary Exchange Networks — and the Sharing Premium ensures that this economic reality is reflected in Quantum Privacy Rewards allocation.

- **Humanity Premium:** Resources, contributions, and Resource Derivatives that measurably advance human welfare — education, workforce development, lifelong learning, public health, clinical research, poverty reduction, food security, housing stability, digital inclusion, indigenous community empowerment and cultural preservation, arts and culture, architectural and historical preservation, and the preservation of human dignity and agency in an era of accelerating automation — earn premium Quantum Privacy Rewards, preferential matching, and stronger Exchange Token flows.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

The Humanity Premium ensures that the QPN/PNX does not merely optimize economic efficiency but structurally rewards contributions that strengthen the human foundations on which a healthy society depends. The architecture also provides a structural safety net: where AI-driven automation or economic disruption displaces individuals or communities, the Humanity Premium ensures that resources directed toward transition support, dignified re-engagement, and inclusive opportunity creation are economically rewarded rather than treated as charitable overhead.

- **Nature Premium:** Resources, Exchange Networks, Resource Pools, and Resource Derivatives governed by Trust Criteria that protect, restore, or sustainably steward natural systems — biodiversity preservation, climate stability, clean water and air, soil health, forests, oceans, and ecological resilience — earn premium Quantum Privacy Rewards, preferential matching, and stronger Exchange Token flows.

  Ecological sustainability is a first-class governance dimension of the Unified Trust Model, with impact metrics — including carbon intensity, water use, toxicity, and biodiversity indicators — incorporated into Proof-of-Trust verification and trust-weight computation. Resources demonstrating positive ecological outcomes receive amplified trust-weights and greater liquidity; resources linked to environmental degradation or externalized ecological harm face reduced matching and compressed Exchange Token generation.

  Nature-based assets — forests, carbon sinks, biodiversity reserves, regenerative agricultural systems — can themselves be tokenized as Resource Pool components, creating a new class of economically productive ecological infrastructure whose governance DNA ensures that downstream Resource Derivatives inherit ecological protection requirements.

- **Innovation Premium:** Markets, networks, AI-driven optimization systems, and established institutional structures tend to over-optimize for short-term returns, overweight proven models and dominant resources, and amplify existing network topologies — systematically underinvesting in the novel, unproven, and disruptive approaches that generate the largest long-run gains.

  The Innovation Premium counteracts this structural bias by rewarding diversity of resources, participants, and approaches: contributions that introduce novel Resource Derivatives, attract participants from underrepresented domains or disciplines, or allocate resources to primary research and scientific inquiry that lacks an established reputation, dominant Trust Authority endorsement, or obvious near-term economic return earn premium Quantum Privacy Rewards, preferential matching, and enhanced Exchange Token flows. The Innovation Premium ensures that the QPN/PNX does not replicate the incumbent-protective dynamics of traditional markets by embedding structural incentives for exploration alongside exploitation.

Governance Premiums and the EP3 Nature & Humanity Trust

The Governance Premiums do not operate solely through Quantum Privacy Rewards allocation and Exchange Token economics. They also directly inform the investment priorities of the EP3 Nature & Humanity Trust, which receives at least 70% of Exchange Root proceeds — expected to grow to over 90% based on stated founder commitments and investor preferences.

The EP3 Trust's investment mandate is structurally aligned with the Governance Premium dimensions:

- **Ecological restoration & climate adaptation** (Nature Premium),
- **Education & workforce development** (Humanity Premium),

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Scientific & medical research** (Safety and Humanity Premiums),
- **Fundamental scientific research & paradigm-shifting innovation** (Innovation Premium),
- **Digital public infrastructure & civic resilience** (Freedom Premium), and
- **Ethical governance innovation** (Ethics Premium).

Unlike traditional philanthropy, the EP3 Nature & Humanity Trust does not spend down principal; it reinvests through PNX market mechanisms — compounding returns through zero-marginal-cost reuse while directing capital toward the governance dimensions the ecosystem is architecturally designed to reward.

The Governance Premiums and the Trust thus form a reinforcing loop: the Premiums create sustained market demand for resources aligned with nature, humanity, safety, freedom, and innovation, while the Trust concentrates long-term capital investment into those same dimensions — ensuring that the economic signals embedded in governance DNA are backed by sustained, compounding institutional commitment.

This creates an incentive for investments and contributions aligned with the Trust's mandate immediately, even before the Trust begins receiving allocations from the Exchange Root — because the Governance Premiums guarantee that resources directed toward these dimensions will attract preferential matching, stronger Exchange Token flows, and higher Quantum Privacy Rewards from the moment the first Exchange Networks begin settling.

4.3 Adaptive Premiums

Adaptive Premiums govern the dynamic regulation and self-correction of the QPN/PNX as it grows. Unlike Launch Premiums, which drive bootstrapping incentives and encourage growth, and Governance Premiums, which embed enduring values into governance DNA, Adaptive Premiums address the inherently unpredictable dynamics of complex system growth — recognizing that even well-designed architectures can generate emergent imbalances, over-amplified feedback loops, and concentration effects that undermine the sustainability, resilience, and fairness the system is designed to produce.

Adaptive Premiums operate as continuous regulatory mechanisms: monitoring system-wide performance, detecting structural imbalances, and adjusting allocation weights, matching priorities, and economic signals to correct deviations before they compound.

- **Proportionality Premium:** Complex networks and AI-driven optimization systems are prone to non-linear feedback loops that can over-amplify early signals — concentrating Quantum Privacy Rewards, routing priority, and network influence in ways that exceed actual incremental value, discourage participation by later entrants, or undermine overall value by prematurely depleting available reward pools.

  The Proportionality Premium provides that Quantum Privacy Reward allocations remain proportional to:

  (1) the incremental value of the verified contribution (i.e., causal impact on activation, settlement, reuse, or risk reduction),

  (2) the scarcity of credible alternative pathways to secure equivalent outcomes (i.e., how replaceable the contribution is at the time it occurs), and

  (3) the effort and risk borne by the contributor in delivering the outcome (including organizational friction, compliance burden, execution risk, and reputational or professional exposure).

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

This principle ensures sufficient incentives to motivate widespread participation, while preventing excessive or unjustifiable windfall rewards driven by path dependence, preferential attachment, or early positional advantage rather than continuing value creation.

Operationally, the Proportionality Premium ensures that QP Reward allocation scales with verified impact rather than with the compounding effects of luck, timing artifacts, or self-reinforcing network position. It functions as a feedback-control layer inside the QP Reward allocation system — preserving strong early incentives where they are truly scarce and high-risk, while preventing early advantage from hardening into permanent dominance.

For example, a person who makes the first introduction in a contribution graph that ultimately leads to a commitment from a hyperscaler could earn extraordinary, life-changing wealth — but the Proportionality Premium ensures that the reward reflects the verified incremental value and scarcity of that contribution rather than compounding indefinitely through path dependence alone. That introduction might make them a multi-billionaire, but not necessarily a trillionaire — not unless they continue to amplify their contribution graph to earn rewards at that scale.

- **Balance Premium:** The Balance Premium monitors the growth and performance of the overall ecosystem and its constituent Exchange Networks, Resource Pools, and Accelerators, identifying where embedded governance DNA, dominant network positions, or concentrated resource flows create systemic imbalances or exploitation that risk undermining sustainability, resilience, equity, or long-run ecosystem health.

  Where imbalances are detected — excessive concentration in a single Exchange Network that undermines efficiency or sustainability, patterns of systemic exploitation, over-reliance on a narrow set of Trust Authorities or Trust Taxonomies, sector-specific dominance that suppresses competitive entry, geographic or demographic exclusion, or governance monocultures that reduce adaptive capacity — the Balance Premium adjusts Quantum Privacy Rewards allocation and Exchange Token economics to favor countervailing contributions: resources from underrepresented domains, participants from underserved jurisdictions, alternative Trust Authority frameworks, and competitive alternatives to dominant nodes.

  The Balance Premium does not impose static quotas or centralized redistribution; it operates through the same market-based, Proof-of-Trust-verified mechanisms as all other Premiums — creating economic incentives for the specific contributions the ecosystem needs most at any given moment to maintain structural health.

4.4 Quantum Genomes: How UTM Premiums Are Embedded, Inherited & Amplified

The Governance Premiums described above are not abstract principles applied after the fact — they are structurally embedded in every layer of the QPN/PNX architecture through the Unified Trust Model's governance machinery, and amplified through inheritance, matching, and evolutionary selection at every stage of resource creation, transformation, and reuse.

To understand how this works, the architecture defines a precise governance vocabulary modeled on molecular biology — not as a loose metaphor, but as a structural analogy that captures how governance content is created, inherited, expressed, regulated, and selected across the Privacy Network ecosystem.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Quantum Genes, Quantum DNA, and Quantum Genomes

Quantum Genes are the smallest heritable units of governance within the Quantum Privacy Network. Each Quantum Gene is an individual UTM element — a specific Trust Criterion, Trust Credential, governance policy, commercial term, implementation specification, privacy requirement, jurisdictional constraint, attribution rule, or safety guardrail — that can be individually active or dormant depending on context. Just as biological genes encode specific proteins or regulatory functions, each Quantum Gene encodes a specific governance behavior: who can access a Resource, under what terms, with what provenance obligations, subject to what regulatory constraints, and with what economic attribution.

Quantum DNA is the UTM content actually expressed in a specific QPC, PPN, QP Resource, Exchange Network, or Resource Pool at any given moment. Quantum DNA determines the entity's current behavior — what it can do, who it can interact with, under what terms, and how value is attributed and settled. Not all Genes available in the entity's Genome are expressed in its DNA at any given time; context determines which Genes are active. The distinction between DNA and Genome is critical: the DNA defines the *phenotype* — the observable expressed traits and behavior — while the Genome is the *genotype* — the complete set of governance possibilities.

Quantum Genomes are the complete ontological frameworks of Trust Authorities and Trust Taxonomies that define the full universe of available Quantum Genes for any given entity. The Genome encompasses everything the entity *could* express — every Trust Criterion it could evaluate, every Trust Credential it could present, every governance policy it could enforce, every jurisdictional adaptation it could make — while the DNA is what it *currently* expresses in its active context. A QPC operating in a healthcare context expresses healthcare-relevant Genes from its Genome; the same QPC interacting with a financial services Exchange Network expresses financial-services-relevant Genes — all from the same Genome, with different Genes active in each context.

Regulatory Genes are the control mechanisms within the Quantum Genome that determine which Quantum Genes are active in different contexts — different jurisdictions, use cases, infrastructure environments, interaction types, and developmental stages of the Privacy Network. Regulatory Genes enable the same Genome to govern a QPC from initial EasyAccess opt-in through full Exchange Network participation, adapting behavior to each context without requiring a new Genome. When a PPN operating under EU jurisdiction interacts with a Resource governed by U.S. healthcare regulations, Regulatory Genes activate the GDPR-relevant and HIPAA-relevant Quantum Genes simultaneously, ensuring both governance regimes are enforced without manual configuration or bilateral negotiation. This is how biological DNA works: regulatory genes (promoters, enhancers, silencers, transcription factors) control which portions of an organism's identical genome are expressed in different cell types, at different developmental stages, and in response to different environmental signals — allowing the same genome to govern a single-celled embryo and a trillion-cell adult. The QPN's Regulatory Genes serve the same function, allowing a single Quantum Genome to govern a newly instantiated PPN and a mature, globally connected Exchange Network.

Parental DNA, Inherited DNA, and the Governance Lineage Chain

Quantum DNA is inherited through two fundamentally different mechanisms, each corresponding to a different context in which new entities emerge within the Quantum Privacy Network. Understanding both is essential to grasping how governance propagates, evolves, and compounds across the ecosystem.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Context 1: The Birth of New Privacy Networks — Two-Parent Inheritance

When the Quantum Privacy Network interacts with an individual or organization outside its existing boundaries — through an EasyAccess opt-in, a direct QPC creation, or any activation event that brings a new participant into the ecosystem — a new PPN or EPN is instantiated. This boundary-crossing event is the QPN's analog to biological sexual reproduction: two parents contribute governance DNA that combines to form a unique new entity.

The **sponsoring PPN or EPN** functions as the ovum — contributing the operational infrastructure and framework genome. Like the biological ovum, which provides not only half the nuclear genome but the entire cellular machinery (mitochondria, ribosomes, endoplasmic reticulum) that allows the organism to function from the moment of fertilization, the sponsoring entity provides both governance DNA and the operational substrate on which that DNA is expressed: the Exchange Provider services the new entity relies upon, the Privacy Domain configurations, the pre-associated Trust Authorities, the default commercial terms, and the Regulatory Genes that govern context-dependent behavior. The sponsor can either serve as the Exchange Provider directly or delegate the implementation of specific services to other Exchange Providers based on terms specified in its DNA — but in either case, the operational infrastructure is inherited maternally.

The **individual person or organization** for whom the PPN is created functions as the sperm — contributing a more compact but equally essential governance identity: the Trust Criteria and Trust Credentials that have accumulated through their prior interactions with the Quantum Privacy Network, their policy decisions and personal preferences, their professional credentials and jurisdictional context, their consent choices and value commitments. Like the biological sperm, this contribution is what makes the new entity genetically unique — what distinguishes it from every other PPN created by the same sponsor.

The **new PPN/QPC** that emerges is the fertilized ovum — a unique entity with Quantum DNA inherited from both parents, running on the sponsor's operational infrastructure while expressing the individual's governance identity. Its Quantum Privacy Domains are always protected by global Trust Authorities that govern Privacy Algorithms and other elements critical to the trustworthiness of the overall network, ensuring that neither parent's DNA can override the universal compliance invariants that protect all participants.

The analogy extends to mitochondrial DNA. In biology, mitochondrial DNA is inherited exclusively from the mother — it passes through the ovum's cellular machinery, not through the sperm. In the QPN, certain infrastructure-level governance content is similarly inherited exclusively from the sponsoring entity: the Exchange Provider configuration, the Privacy Domain cryptographic parameters, the foundational Trust Authority associations. This is the QPN's mitochondrial DNA — the operational substrate that the individual benefits from but does not directly modify, inherited through the maternal line of sponsoring PPNs and EPNs. Just as an organism's mitochondrial lineage can be traced back through an unbroken maternal chain, a PPN's infrastructure lineage can be traced back through its chain of sponsoring entities to the founding Exchange Providers.

Like a biological organism, the new PPN begins growing and differentiating immediately — accumulating new Quantum Genes through interactions, activating different Regulatory Genes in different contexts, and eventually becoming capable of sponsoring the creation of new PPNs itself, passing its own evolved governance DNA — now a combination of both parents' contributions and the Genes acquired through its own development — forward to the next generation.

Context 2: The Creation of Resource Derivatives — Multi-Parent Recombination

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

A fundamentally different inheritance pattern emerges when existing QP Resources are combined and reused within the QPN to create Resource Derivatives. Where PPN creation involves two parents producing a unique offspring, Resource Derivative creation involves potentially hundreds or thousands of input Resources — each contributing its own Quantum DNA to the resulting derivative.

The biological analog shifts from sexual reproduction to something closer to **polygenomic recombination** — a process with parallels in horizontal gene transfer (where bacteria incorporate genetic material from many unrelated organisms, acquiring capabilities their own lineage never evolved), and in **symbiogenesis** (where entirely separate organisms merge their genomes permanently, as when ancient free-living bacteria were incorporated into eukaryotic cells to become mitochondria and chloroplasts — creating a fundamentally new class of organism with capabilities neither ancestor possessed alone).

When an Exchange Network combines clinical trial data (governed by HIPAA, informed consent, and IRB oversight), financial claims records (governed by SOX, PCI-DSS, and payer contracts), genomic sequences (governed by genetic privacy laws and research ethics frameworks), geolocation data (governed by GDPR and state privacy laws), and computational infrastructure (governed by cloud provider terms and security accreditation) into a composite analytics Resource Derivative, the derivative inherits the complete Quantum DNA of every input — every Trust Criterion, every governance constraint, every commercial term, every attribution obligation, every regulatory requirement from every source. This inheritance is comprehensive and non-negotiable: the derivative cannot shed the governance constraints of any parent Resource, no matter how many parents contributed.

But while all Inherited DNA is preserved and enforced, not all of it needs to be expressed simultaneously. The Exchange Network or Resource Pool that creates the derivative acts as the **Regulatory Gene environment** — specifying which Quantum Genes are actively expressed to define the derivative's phenotype for its intended market or purpose. A healthcare analytics derivative might express the clinical relevance Genes, the privacy protection Genes, and the outcome quality metric Genes, while the financial governance Genes, the geolocation privacy Genes, and the infrastructure security Genes remain enforced but dormant in that context — ready to activate the moment the derivative enters a context where those constraints become relevant.

The mitochondrial DNA analog operates in this context as well, with consistent architectural meaning across both inheritance patterns. Just as the sponsoring entity's Privacy Domain infrastructure serves as mitochondrial DNA in PPN creation, the Privacy Domain within which the Resource Derivative is generated — its Exchange Provider governance, its Privacy Algorithm configuration, its computational environment, and its enforcement mechanisms — serves as the mitochondrial DNA of the derivative. The derivative runs on that domain's operational infrastructure regardless of which input Resources contributed governance DNA to it, just as every biological cell runs on its mitochondria regardless of which nuclear genes are expressed. Mitochondrial DNA thus has a single, consistent meaning throughout the QPN: it is always the operational substrate inherited from the environment within which the new entity was created — not from the genetic parents themselves. The parents contribute what the entity *is*; the environment contributes what the entity *runs on*.

This selective expression is what makes Resource Derivatives commercially viable despite their potentially enormous Inherited DNA burden. A derivative carrying the governance DNA of a thousand input Resources would be unusable if every Gene had to be actively satisfied in every context. Instead, the Regulatory Gene environment curates the expressed DNA to optimize market fit, reuse efficiency, and demand matching — while the full Inherited DNA

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

remains cryptographically bound in the Trust Block lineage, available for enforcement whenever any dormant constraint becomes contextually relevant.

The two inheritance contexts differ in what Regulatory Gene selection is optimizing for. In **PPN creation**, Regulatory Genes adapt the new entity to the individual's context — their jurisdiction, their professional role, their developmental stage, their personal preferences. The optimization is person-centered. In **Resource Derivative creation**, Regulatory Genes adapt the derivative to market demand — making it attractive, interoperable, and useful for specific Exchange Networks, Solution Providers, or use cases. The optimization is market-centered. But in both cases, the underlying mechanism is identical: Regulatory Genes selecting from a rich Quantum Genome which Genes to express in a given context, while the complete Inherited DNA remains preserved, enforced, and available.

As the PPN grows and interacts with other QPCs, its DNA evolves — incorporating new Genes from the Genomes of entities it interacts with, adopting new Trust Authorities, activating dormant Regulatory Genes — while the Parental DNA from both parents is preserved as provenance in the Trust Block lineage. When that PPN later sponsors the creation of another PPN through an EasyAccess interaction, its own DNA — now a combination of both parents' original contributions and the Genes acquired through its own development — becomes the maternal Parental DNA of the new child entity. The grandparents' DNA is preserved in the Trust Block lineage, creating multi-generational governance provenance that is cryptographically auditable back to the founding Trust Blocks.

Multi-Genome Individuals: Adaptive Identity Across Contexts

The biological analogy, powerful as it is, actually understates what the QPN architecture enables. In biology, every organism is locked into a single genome for life. A bird cannot become a fish; a human cannot grow wings to fly and then switch to gills to breathe underwater. Biological organisms are permanently committed to the DNA they inherited at conception.

In the QPN, individuals face no such constraint. Because any person can operate an arbitrary number of PPNs and QPCs simultaneously — creating new ones at any time, through any EasyAccess interaction, supported by any Exchange Provider — each individual can maintain a *portfolio* of Privacy Networks, each with its own distinct Quantum Genome optimized for a specific context or purpose.

A person might maintain one PPN with a Genome optimized for workplace interactions — emphasizing professional credentials, enterprise compliance frameworks, and employer-compatible commercial terms. A second PPN with a Genome optimized for healthcare — emphasizing patient rights, clinical data governance, informed consent frameworks, and health-outcome attribution. A third optimized for personal finance — emphasizing KYC/AML compliance, transaction privacy, and investment-grade audit standards. A fourth for creative work — emphasizing intellectual property protections, attribution chains, and content licensing terms. A fifth for civic participation — emphasizing government transparency requirements, public benefit allocation, and democratic accountability.

Each PPN has its own Quantum DNA — its own expressed governance traits and behavior — drawn from its own Quantum Genome. The individual, or AI agents acting on their behalf, chooses which PPN governs each interaction, which PPN publishes each Resource, and which PPN routes each activity. It is as though a person could grow wings and fly when they need to cross a mountain, then switch to gills and breathe underwater when they reach the ocean — carrying both genomes simultaneously and switching between them as context demands.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

This architectural property has profound consequences for evolutionary selection within the PNX. Because individuals control which PPNs they rely upon for specific activities — for publishing Resources they have rights to, for governing interactions that emerge from their online behavior, for routing activity through specific Exchange Providers — there is intense competitive pressure on the Quantum DNA and Genomes offered by sponsoring entities. PPNs whose DNA offers unfavorable commercial terms, weak privacy protections, poor Exchange Provider performance, or governance constraints that limit reuse and settlement will find themselves progressively abandoned as individuals route activity through more favorable alternatives. This reduces the QP Rewards derived from PNX Settlement flowing through the disfavored PPN (since settlement emerges from QP Resource contributions governed by that PPN's DNA), and it also reduces that PPN's reproductive rate — it will generate fewer new PPNs and QPCs, since these emerge as a byproduct of online interactions that are governed by the user's behavioral choices and PPN routing preferences.

The result is natural selection operating through individual choice: PPNs with attractive, well-aligned Quantum DNA reproduce prolifically (generating downstream PPNs through every interaction they govern), while PPNs with unattractive DNA are starved of both settlement value and reproductive opportunity. This creates the same evolutionary pressure toward UTM Premium alignment that operates at the Resource level, but applied to the Privacy Networks themselves — ensuring that the infrastructure layer, not just the content layer, evolves toward governance excellence.

Surpassing Biology: Lamarckian Evolution and Living Governance

The QPN's governance evolution surpasses its biological analog in one final, critical respect. In biology, DNA is fixed at conception. An organism cannot rewrite its own genome in response to experience — it can only pass on what it inherited, with occasional random mutations. Biological evolution is strictly Darwinian: organisms cannot acquire new traits during their lifetime and transmit them to offspring.

The QPN's Quantum DNA and Quantum Genomes have no such limitation. A QPC can adopt new Trust Authorities at any time, incorporating entirely new Trust Taxonomies into its Genome. It can activate dormant Regulatory Genes in response to entering a new jurisdiction or engaging with a new market. It can modify its expressed DNA — changing its governance behavior — without disrupting its identity, its provenance chain, or its compliance continuity. And crucially, when that evolved QPC sponsors the creation of new PPNs, or when its Resources are reused to create Resource Derivatives, the acquired governance characteristics are inherited by the next generation.

This is Lamarckian evolution — the inheritance of acquired characteristics — which biology cannot support but the QPN architecture implements by design. A PPN that develops sophisticated healthcare governance through years of clinical research participation passes that governance maturity directly to every PPN it sponsors and every Resource Derivative it produces. Governance improvements propagate forward immediately, without waiting for the slow Darwinian process of random variation and selection.

The combined effect is an evolutionary system that operates at extraordinary speed: Darwinian selection eliminates governance configurations that the market rejects, while Lamarckian inheritance propagates governance configurations that the market rewards. Both DNA and Genomes can dynamically evolve throughout an entity's lifetime without killing the organism — enabling continuous adaptation, context-switching, and governance improvement that compounds across every generation of the Privacy Network ecosystem.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Individual Autonomy: Controlling Your Own Genetic Destiny

The Quantum DNA framework gives every person something that no prior digital architecture — and no biological system — has offered: genuine individual autonomy over their governance experience, combined with the ability to participate safely in a global trust-enforced ecosystem without requiring agreement, mutual trust, or even awareness of the other participants.

Adults always retain the ability to override or customize the Trust Criteria and Quantum DNA that influence their personal online experiences within their own PPNs. A person who dislikes the content-filtering policies embedded in one PPN's DNA can adjust them. A person who wants stricter privacy protections than the default can activate additional Regulatory Genes. A person who prefers different commercial terms can switch to a PPN whose Parental DNA reflects their preferences, or modify the DNA of an existing PPN. The sole constraint is that individuals cannot alter the commercial terms or compliance requirements of QP Resources they rely upon — the Inherited DNA of Resources contributed by others remains inviolate, because those constraints protect the rights, privacy, and economic interests of the upstream contributors. You control your experience; you cannot unilaterally change what you owe to others.

Children can similarly specify their preferences within their own PPNs, subject to the supervision and control of their parents or guardians, and to child-protection and safety policies defined by the Exchange Networks or Resource Pools they interact with. The Regulatory Gene framework handles this naturally: a child's PPN includes Regulatory Genes that activate parental oversight Trust Criteria — governing what content is accessible, what interactions are permitted, what Resources can be published, and what commercial terms apply — with those Regulatory Genes deactivating progressively as the child reaches developmental milestones or legal thresholds defined in the applicable Trust Taxonomy. This mirrors how biological regulatory genes govern developmental stages, but with a crucial advantage: the governance boundaries are set by the family and reinforced by the ecosystem's safety infrastructure, rather than imposed unilaterally by a platform, an algorithm, or a government — and they adapt continuously as the child matures rather than operating as blunt age-gate cutoffs.

This parent-child supervisory model is actually one instance of a general delegation pattern that the Quantum DNA framework supports across every professional, organizational, and human-machine relationship.

Delegated Authority in Professional and Organizational Contexts

In professional settings, a manager might grant staff members PPNs or QPCs that inherit the manager's enterprise authorities — access to company funds, procurement systems, vendor relationships, customer data — but with Regulatory Genes that impose approval thresholds, spending limits, and audit requirements. A staff member can autonomously execute transactions below a specified level, while transactions above that threshold activate Regulatory Genes requiring the manager's explicit approval before the Trust Block is committed. The manager's oversight is structural, not procedural — it is encoded in the Quantum DNA of the delegated PPN, enforced cryptographically, and auditable through the Trust Block lineage. The manager can adjust these thresholds at any time by modifying the Regulatory Genes, expanding or contracting the delegation as trust is earned or circumstances change.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

A physician provides an even richer example. A doctor operates within a complex web of authorities and responsibilities: HIPAA treatment, payment, and operations authority over patient records; prescribing privileges governed by DEA registration and state medical board licensing; clinical decision-making authority subject to institutional protocols and malpractice standards; billing authority subject to payer contracts and fraud-prevention requirements. The doctor's PPN encodes all of these as Quantum DNA, with Regulatory Genes adapting which authorities are active depending on context — inpatient vs. outpatient, emergency vs. routine, research vs. clinical care.

The doctor can then extend her authorities to a network of staff — nurses, medical assistants, billing coordinators, referral specialists — each receiving a PPN whose Parental DNA inherits specific subsets of the doctor's authorities. A nurse's PPN might inherit the authority to access patient records and document clinical observations, but with Regulatory Genes that require the doctor's approval before modifying treatment plans or ordering high-risk medications. A billing coordinator's PPN might inherit the authority to submit claims and manage prior authorizations, but with Regulatory Genes that flag unusual billing patterns for the doctor's review. Each delegate operates autonomously within their DNA-defined scope, while the doctor retains oversight through Regulatory Gene-enforced approval gates — and everything remains the doctor's responsibility, because the Trust Block lineage traces every delegated action back to the doctor's authority.

AI Agents and the Governed Autonomy Model

The most consequential application of this delegation pattern is the relationship between humans and AI agents — and this is where the Quantum DNA framework addresses what may be the defining governance challenge of the coming decades.

The core problem of agentic AI is this: how do you let an AI agent act autonomously — making decisions, executing transactions, accessing sensitive data, interacting with other agents and humans — while ensuring that a responsible human remains meaningfully in control? Today's approaches are crude: either the AI operates with broad permissions and the human trusts it not to misbehave (unsafe at scale), or every consequential action requires explicit human approval (defeats the purpose of autonomy). Neither approach scales.

The QPN's Quantum DNA framework provides a structural solution. Every AI agent operates within a PPN whose Quantum DNA defines precisely what the agent is authorized to do. The agent's PPN inherits Parental DNA from the human (or organization) that created it, establishing the scope of its delegated authority. Regulatory Genes within that DNA define a granular, context-sensitive governance boundary:

- **Autonomous zone:** Actions that fall within well-defined parameters — routine data retrieval, standard formatting, low-stakes scheduling, information synthesis below a sensitivity threshold — execute without human intervention. The Trust Block records the action, the authorization basis, and the provenance, but no approval gate is triggered.
- **Supervised zone:** Actions that cross defined thresholds — accessing sensitive records, committing financial resources, communicating with external parties, modifying shared Resources, making clinical or legal recommendations — activate Regulatory Genes that require the supervising human's approval before the Trust Block is committed. The agent proposes the action; the human reviews and authorizes; the Trust Block records both the proposal and the authorization, creating an immutable audit trail of the human-agent collaboration.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Prohibited zone:** Actions that exceed the agent's delegated authority entirely — the Quantum DNA simply does not contain the Genes required to attempt them, or Regulatory Genes unconditionally block execution. An AI agent operating under a doctor's delegated authority cannot prescribe controlled substances if the doctor's delegation DNA does not include DEA prescribing Genes, regardless of what the agent's underlying model might be capable of.

This three-zone model scales naturally with trust, context, and capability. A new AI agent starts with a narrow autonomous zone and broad supervised zone — the human approves most actions while the agent builds a Quantum Reputation through its Trust Block history. Crucially, an agent's Quantum Reputation is not confined to a single person's PPNs — it accumulates across the full population of PPNs the agent operates within and across every context it encounters, creating a portable, verifiable track record that any supervising human or organization can evaluate. A doctor considering whether to delegate clinical triage to an AI assistant can assess that agent's Quantum Reputation across thousands of prior clinical interactions supervised by other physicians, in multiple specialties and jurisdictions — not just its performance within her own practice. As an agent demonstrates reliability across this broader population, the autonomous zone can widen through two complementary mechanisms: the supervising human can directly modify Regulatory Genes based on their own experience and judgment, and Trust Authorities can update the Trust Credentials and Trust Criteria governing the agent's PPN to reflect the accumulated evidence and validation embedded in its Quantum Reputation — automatically activating Regulatory Genes that expand the agent's delegated authority as defined thresholds of demonstrated competence, consistency, and safety are met across diverse real-world conditions. This means governance boundaries evolve based on verifiable evidence rather than blanket permission, individual intuition, or narrow single-context testing — and the evolution can be both locally directed (by the supervising human) and systemically informed (by Trust Authorities whose credentialing standards reflect population-wide performance data). If the agent makes errors or exhibits unexpected behavior, both mechanisms work in reverse: the human can narrow the autonomous zone instantly by activating additional Regulatory Genes, and Trust Authorities can downgrade the agent's Trust Credentials — propagating that negative signal through the Quantum Reputation and tightening governance boundaries across every PPN the agent operates within, informing every other supervisor's trust calibration in turn.

Critically, this governance is not enforced by the AI model itself — it is enforced by the Quantum Privacy infrastructure surrounding the agent's PPN. The agent cannot override its own Regulatory Genes any more than a biological cell can rewrite its own regulatory DNA. The governance boundary exists at the architectural level, not the application level, which means it is resilient to prompt injection, jailbreaking, model misalignment, or any other failure mode that operates within the agent's computational environment. The Trust Block that authorizes each action is generated by the Privacy Domain infrastructure, not by the agent — creating a separation of concerns between the agent's intelligence (what it wants to do) and the governance layer (what it is permitted to do).

The delegation can also be multi-level: a doctor delegates to an AI clinical assistant, which in turn delegates specific subtasks to specialized AI agents — a lab-ordering agent, a prior-authorization agent, a patient-communication agent — each with its own PPN inheriting progressively more specialized Parental DNA. The lab-ordering agent can access the patient's relevant lab history and place routine orders autonomously, but activates Regulatory Genes requiring the clinical assistant's review for unusual combinations, and the doctor's approval

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

for high-cost or high-risk orders. Each level of delegation narrows the scope while preserving the audit chain back to the responsible human.

This architectural pattern applies uniformly across every domain: a financial advisor delegating to AI trading agents with position-size limits and compliance-triggered approval gates; a corporate general counsel delegating to AI contract-review agents with authority to approve standard terms but escalation requirements for non-standard provisions; a supply-chain manager delegating to AI procurement agents with autonomous purchasing within approved vendor lists and budget thresholds. In every case, the Quantum DNA of the agent's PPN defines the delegation scope, the Regulatory Genes define the approval boundaries, the Trust Block lineage provides the audit trail, and the Inherited DNA of every Resource the agent touches ensures that upstream compliance and commercial obligations are preserved regardless of how many levels of delegation the action has passed through.

The result is a governance framework for agentic AI that is simultaneously permissive (agents can act autonomously within their DNA-defined scope), safe (humans retain structural control through Regulatory Genes that cannot be overridden by the agent), accountable (every action is recorded in an immutable Trust Block lineage traceable to the responsible human and agents), and adaptive (the governance boundary evolves with demonstrated capability rather than requiring static permission sets).

The Architectural Consequence: Autonomy Without Agreement

The common thread across all of these delegation patterns — parent-child, manager-staff, doctor-delegate, human-AI agent — is that the Quantum DNA framework enables autonomy without requiring agreement.

Every person controls their own personal experience. Every delegate operates within DNA-defined authority. Every AI agent acts within governance boundaries it cannot override. No one needs to agree with anyone else's choices, because trust is structural — built into the architecture through Quantum Privacy, Proof of Trust, and the Unified Trust Model — rather than interpersonal. Individuals can voluntarily associate with whomever they want, and can safely allow their Resources to be pooled and reused on a global scale — even with people, organizations, and AI agents they don't know or necessarily trust — because the Trust Blocks, Inherited DNA, and Regulatory Genes ensure that every interaction respects every participant's governance constraints without requiring negotiation, reconciliation, or mutual awareness.

People don't need to agree. They need to participate. The architecture handles the rest.

The Four-Layer Mechanism: Embedding, Inheritance, Selection, and Adaptation

The mechanism through which Quantum Genomes propagate and amplify UTM Premium alignment operates through four interlocking layers:

- **Embedding:** Exchange Networks and Resource Pools incorporate UTM elements — Trust Credentials, Trust Criteria, and governance policies — drawn from common Trust Authorities and Trust Taxonomies that facilitate semantic interoperability and ongoing cross-organizational, cross-industry, and cross-jurisdictional reuse. These elements define how Resources are transformed, what Quantum Ratings or Quantum Reputations

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

are required to authorize access, how Resources are matched to demand (including priority among alternative Resources), and what terms govern the resulting Resource Derivatives — including commercial terms and revenue sharing, authorized recipients and counterparties, authorized purposes of use, regulatory and privacy requirements, jurisdictional constraints, data retention and revocation policies, safety and ethical guardrails, attribution and provenance obligations, and every other dimension necessary to ensure alignment with the UTM Premiums. Privacy Networks acting as Resource, Exchange, Solution, or Engagement Providers can systematically embed matching and reuse policies that prioritize how they discover Resources when growing Resource Graphs to meet demand, and what they make visible to other Exchange Networks, Resource Pools, or Solution Providers.

- **Inheritance:** Every Resource Derivative inherits the Quantum DNA embedded in the Trust Blocks of its upstream Resources — and this inheritance is comprehensive and non-negotiable. A Resource Derivative cannot shed the governance constraints of its parent Resources any more than an organism can shed its genetic code. When an Exchange Network combines clinical data governed by HIPAA-derived Trust Criteria with genomic data governed by informed-consent Trust Criteria, the resulting Resource Derivative inherits both sets of constraints, and every subsequent derivative inherits from it in turn. This creates multi-generational governance lineage in which the UTM Premium alignment embedded at the point of resource creation propagates forward through every reuse, transformation, and recombination event — compounding governance alignment across the ecosystem over time. Critically, while all Inherited DNA is enforced, the Exchange Network or Resource Pool that creates the derivative can specify which Quantum Genes are *expressed* — curating the active DNA to optimize market fit, reuse efficiency, and demand matching, provided no inherited constraint is violated.

- **Selection:** Selection operates at multiple levels simultaneously. At the **Resource level**, Resources whose Quantum Genomes are well-aligned with the UTM Premiums — reflecting high ethics, strong reputation, robust safety, broad sharing, and genuine innovation — are preferentially matched, more frequently reused, and generate stronger Exchange Token flows. Resources with incompatible governance DNA are progressively excluded from reuse and PNX settlement, because the Resource Derivatives they produce are either incompatible with the broader ecosystem (and therefore cannot be reused or recombined), or they damage the Quantum Ratings and Quantum Reputations of the Exchange Networks and Resource Pools that incorporate them — reducing those networks' PNX settlement participation and economic returns. Quantum Genomes that are compatible with the prevailing Trust Taxonomies can interbreed and reproduce successfully across Exchange Networks and Resource Pools, while governance Genomes that are incompatible cannot produce viable Resource Derivatives and are progressively eliminated from the population. At the **Privacy Network level**, individuals choosing among their portfolio of PPNs exert continuous selection pressure on the Quantum DNA offered by Exchange Providers and sponsoring entities — routing activity, Resources, and reproductive interactions toward PPNs with the most favorable governance, and starving disfavored PPNs of both settlement value and downstream network formation.

- **Adaptation:** By aligning with common Trust Authorities and Trust Taxonomies that maximize interoperability and reuse, Exchange Networks and Resource Pools naturally aggregate into interconnected networks with compatible Quantum Genomes. This layered aggregation creates a network of networks whose governance content is mutually reinforcing — amplifying the UTM Premiums through scale effects and network density. At

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

the PNX level, the EasyAccess Authorization Network governs visibility and matching across the entire Privacy Network Exchange based on the Unified Trust Model and Proof of Trust, providing an efficient and robust mechanism for aligning market outcomes to the UTM Premiums at a global scale across all participants. Because both DNA and Genomes can evolve dynamically — through Lamarckian inheritance of acquired governance characteristics, through multi-Genome individual choice, and through Darwinian selection at every level — this adaptation operates at extraordinary speed, compounding governance quality across every generation of the ecosystem.

Because individuals and enterprises have freedom of choice — they can rely upon any Trust Criteria, Trust Authorities, and Trust Taxonomies they prefer, and individuals can maintain multiple PPNs with distinct Genomes optimized for different contexts — the Quantum Genome is not imposed from above but selected from below. Participants who adapt their Quantum Genomes to align with the UTM Premiums maximize the value of their Resources within the PNX, because alignment increases matching frequency, reuse density, and Exchange Token settlement. Participants who choose Quantum Genomes that diverge from the UTM Premiums find their Resources progressively marginalized — not through censorship or exclusion, but through the natural market dynamics of reduced matching, lower reuse, and weaker settlement flows.

The result is a system that responds rapidly and efficiently to realign with the UTM Premiums across different contexts and over time. The Premiums do not need to be centrally enforced — they are emergent properties of a market in which governance alignment is the primary determinant of economic success. The founding choices made during the Accelerator incubation phase — which Trust Authorities are developed and adopted first, which Trust Taxonomies are authored, which Trust Criteria are embedded in founding Resource Derivatives — determine the initial governance Genome of the PNX-settled economy. The evolutionary dynamics ensure that this Genome is continuously refined, adapted, and amplified as the ecosystem grows.

4.5 Privacy Network Provider Roles

Any individual, enterprise, governmental entity, joint venture, or collaborative can participate in the Privacy Network Exchange by serving as a Privacy Network Provider (PNP) in one or more of five distinct roles:

- **Resource Providers** contribute assets, enabling resources, and data;
- **Exchange Providers** enable Privacy Network infrastructure;
- **Exchange Networks** combine and transform Resources into value-added Resource Derivatives;
- **Solution Providers** compose Resources into customer-facing products and services; and
- **Engagement Providers** drive adoption, enrollment, and ongoing participation.

These roles are not mutually exclusive — a single participant can simultaneously serve in any combination of roles, across different use cases, industries, jurisdictions, or on behalf of different participants, through one or more Personal or Enterprise Privacy Networks. Any role can be delegated to other Privacy Network Providers in exchange for a share of the resulting Exchange Token flows, enabling participants to leverage specialized capabilities without building them in-house.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Rights to revenue, Resource Derivatives, and tokenized value generated through PNX activity are allocated based on verified engagement, authorized resource contributions, and demonstrable value creation — as recorded through Quantum Privacy Cells and governed by the Unified Trust Model and Proof of Trust frameworks.

Resource Providers

A Resource Provider is any participant that contributes tangible or intangible resources — data, software, AI models, compute infrastructure, professional services, content, intellectual property, contractual rights, brands, relationships, engagement, governance frameworks, or any other asset — to the Privacy Network Exchange or any affiliated Accelerator, Exchange Network, or Resource Pool.

Resources are connected to the PNX through dual-use infrastructure (existing enterprise platforms such as Databricks, Snowflake, Salesforce, or cloud services) or through Privacy Network-native systems such as EasyAccess Links, EA Consent APIs, or other Unified Trust Model-compliant interfaces. Once connected, a Resource may be made available for dual-use commercialization through existing licensing or revenue-sharing agreements, or tokenized within the PNX as a Resource Token (RT) or aggregated into a Resource Pool Token (RPT) to enable privacy-preserving access, reuse, and derivative value creation across multiple participants.

Resource Providers earn the 70% Resource Provider share of Exchange Tokens generated when their Resources are utilized through the PNX settlement waterfall. The Resource remains fully governed by its originating licensing, compliance, and ownership terms while becoming discoverable, auditable, and monetizable via the Privacy Network Exchange. Because Resources can be reused and recombined repeatedly at zero marginal cost, a single Resource contribution can generate a compounding stream of Exchange Token settlement over time.

Exchange Providers

An Exchange Provider is any participant that establishes or operates the Privacy Network infrastructure through which Resources are published, settled, and governed. Exchange Providers deliver the specialized infrastructure, policy enforcement, and governance capabilities that enable secure, privacy-preserving value exchange across multiple Resource Providers, Solution Providers, and participants.

Exchange Providers are bound to Privacy Networks — every Personal Privacy Network and Enterprise Privacy Network has an associated Exchange Provider. Exchange Providers may acquire their role **explicitly** (through enterprise contracts or Proof of Trust Accreditation), **implicitly** (through EasyAccess engagement that creates PPNs, where the Engagement Provider that initiated the opt-in becomes the default Exchange Provider), or through **self-service** (where an enterprise operates as its own Exchange Provider using its existing dual-use infrastructure).

End users may not be aware of the identity or role of the Exchange Providers associated with their various PPNs, but the commercial terms of each are discoverable — particularly by AI Agents operating on behalf of individuals — creating competitive pressure among Exchange Providers to offer favorable terms in order to retain routing preference across the individual's portfolio of PPNs.

Exchange Providers earn the 30% Exchange Provider share (Exchange Fees) of Exchange Tokens generated by settlement activity flowing through the Privacy Networks they serve. Exchange Providers can selectively allocate a portion of their Exchange Fees to the owners of the Privacy Networks they enable — either as Quantum Privacy Rewards through loyalty

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

programs, as negotiated revenue-sharing arrangements, or as competitive incentives to attract and retain routing preference. They can also delegate the implementation of Exchange Provider services to other vendors or specialized providers, retaining a share of the Exchange Fees and passing the remainder to the delegate.

Individuals can also serve as Exchange Providers — either for themselves or for others whom they enrolled in Personal Privacy Networks through EasyAccess engagement — retaining a portion of the Exchange Fees and either paying vendors to provide the Exchange Provider enablement or delegating to other Exchange Providers on agreed terms.

Over time, each individual and enterprise builds a growing network of PPNs — created automatically through their interactions with other individuals and expanded virally as those individuals' downstream online interactions trigger further PPN activations — earning settlement value as the default Exchange Provider for every PPN they originated, even when those PPNs are subsequently used by other Exchange Networks and services they have no direct relationship with. Individuals can concurrently use many PPNs or create additional PPNs supported by competing Exchange Providers at any time, ensuring that no single enterprise or individual achieves lock-in.

Exchange Networks

An Exchange Network is a governed marketplace within the overall Privacy Network Exchange that connects Solution Providers, Resource Providers, Exchange Providers, and Engagement Providers through agreements that govern how Resources are recombined, reprocessed, and syndicated into value-added Resource Derivatives.

Exchange Networks perform a distinct value-transformation function: they combine and transform input Resources into Resource Derivatives that are worth more than their inputs, contracting with participating Resource Providers to specify the allocation of rights to those derivatives among the input Resources and the Exchange Network itself. The transformation is performed by Resources that are either proprietary to the Exchange Network or contracted for via the PNX. Exchange Networks can also contract with Resource Providers to pool and distribute Resources in accordance with specified terms and to transform them into Resource Derivatives, which can themselves be pooled and distributed.

An Exchange Network may utilize and be linked to one or more Resource Pools, and because Resources and Resource Derivatives can be reused and monetized repeatedly, the Resource Pools associated with an Exchange Network represent a valuable and growing asset that is a primary driver of the Exchange Network's market value and its MUM (Monetization Uplift Multiple).

Governance of Exchange Networks is anchored by the Unified Trust Model and enforced through Proof of Trust. Each Exchange Network defines its own commercial and governance terms, and the Exchange Network itself can be treated as a PNX Resource, with a distinct identity, anchored in a Privacy Domain, and with its own Exchange Network Token (ENT), enabling decentralized ownership, participation, and revenue sharing. ENT holders receive a share of the Exchange Tokens generated by settlement activity within the Exchange Network, proportional to their holdings.

Multiple Exchange Networks can operate in parallel across industries, geographies, or functions, and can contract with each other to form interconnected networks of specialized Exchange Networks through shared Resource Pools and common Trust Authorities and Trust Taxonomies. This federated structure enables market-focused, resource-focused, or jurisdiction-focused Exchange Networks to maintain their specialized depth and competitive

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

advantage while accessing the broader scale and resource diversity of the interconnected network.

Because Resources and Resource Derivatives that are contributed to shared Resource Pools can be reused across all participating Exchange Networks at zero marginal cost, this interconnection increases the Monetization Uplift Multiple (MUM) for every participating Exchange Network — each gains access to a larger resource base and settlement volume without diluting its domain expertise or governance focus. The result scales the Privacy Network Exchange into a unifying global framework for resource pooling, reuse, and value creation in which specialization and scale are complementary rather than competing strategies.

Solution Providers

A Solution Provider is any individual, enterprise, organization, joint venture, collaborative, or team that composes QP Resources into outward-facing Solutions that deliver value to end users, customers, or beneficiaries. A Solution Provider may be a single entity or a multi-party collaboration whose participants contract and hold rights through their respective Quantum Privacy Cells — which function simultaneously as anonymous legal entities (Delaware Series LLCs or jurisdictional equivalents) and as Quantum Privacy Domains — enabling frictionless, privacy-preserving reuse and sharing of resources across organizational boundaries. The participants' respective economic rights and governance roles are governed by the Trust Blocks and Resource Pool terms that structure the collaboration, with all contractual obligations anchored in Inter-QPC Agreements, which are anonymously enforceable through the Unified Trust Model. Solution Providers are the demand-generation layer of the Privacy Network Exchange: they convert Resources that would otherwise sit idle in Resource Pools into revenue-generating products and services by making composition, personalization, pricing, and distribution decisions that create value exceeding the sum of the underlying Resource inputs.

Solution Providers perform the customer-facing extension of the Exchange Network's value-transformation function. Where Exchange Networks compose, transform, and recombine Resources into Resource Derivatives internally, Solution Providers package those derivatives into outward-facing products and services that contract with end users for commercial and usage terms. Solution Providers may also operate entirely within the Privacy Network Exchange, providing services to other Privacy Network participants and receiving payment in Exchange Tokens — convertible to fiat currency, digital assets, or other resources via Quantum Privacy Liquidity Pools, or retained as economic rights that appreciate as the Exchange Networks they participate in grow. The revenue generated by Solution activity flows into the PNX settlement waterfall, creating the Exchange Token distributions that compensate all upstream Resource Providers and Exchange Providers. Without Solution Providers, the value created by Exchange Networks remains latent — it is Solution Provider activity that converts Resource Derivatives into revenue and drives the settlement events that fund the entire ecosystem.

A Solution Provider's economic rights are represented through the existing token taxonomy: Resource Tokens (for the composite Solution itself), Resource Pool Tokens (for the collaborative Resource Pools backing it), and Exchange Network Tokens (for the Exchange Networks whose transformation capabilities and pool assets underpin the Solution). The combination of these token types fully captures the Solution Provider's economic position.

Solution Providers can be implemented as specialized Exchange Networks with customer-facing distribution capabilities, and/or as specialized Resource Pools whose governance

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

terms define customer-contracting, pricing, and revenue allocation. This architectural flexibility means that Solutions can be incubated within Accelerators, formed independently by entrepreneurial participants, or assembled collaboratively across multiple Exchange Networks and Resource Pools.

Solution Providers operate along a spectrum from dual-use to native Quantum Privacy implementations. Existing businesses can serve as dual-use Solution Providers, contracting through the PNX for access to enabling Resources and/or user engagement, in exchange for payments and/or rights to Resource Derivatives. In the dual-use case, only the value of the enabling Resources consumed through the PNX is settled via Exchange Tokens; the Solution Provider's overall customer revenue remains outside the PNX settlement perimeter. By contrast, a native Quantum Privacy Solution is one that is entirely implemented and distributed via the PNX based exclusively on QP Resources, in which case all revenue flows through the PNX settlement waterfall. The dual-use model provides the on-ramp; over time, competitive pressure and superior economics drive migration toward native implementations where the full revenue stream flows through the settlement waterfall.

Solutions are subject to Quantum Ratings and Proof of Trust Accreditation, like any other QP Resource, creating competitive pressure among Solution Providers to optimize for value delivery rather than rent extraction.

Engagement Providers

An Engagement Provider is any participant that drives adoption, enrollment, and ongoing engagement with the Privacy Network Exchange — generating the user interactions, content distribution, and relationship formation that expand the reachable Privacy Graph and create the population-scale participation necessary for PNX settlement to reach critical mass.

Engagement Providers operate through any channel that reaches end users and potential participants: social media, content creation, messaging, apps, websites, influencer networks, advertising, community organizing, affiliate marketing, customer service, or any other mechanism that drives awareness and participation.

Critically, Engagement Providers can drive growth before the full Privacy Network infrastructure is operational — by building awareness and participation in the Quantum Privacy Catalyst Network, they grow the contribution graphs that provide the resources to bootstrap the development of the QPN/PNX itself. Catalyst participation is the egg from which the chicken hatches — the PPNs, Exchange Networks, Privacy Network Exchange, and the privacy-preserving services they collectively enable all emerge from the ecosystem that Engagement Providers help build during the pre-infrastructure phase.

As the ecosystem matures, Engagement Provider activity expands to drive EasyAccess enrollment, PPN activation, and ongoing utilization of Privacy Network-enabled services. When an Engagement Provider's activity results in a new PPN activation, the Engagement Provider (or the entity on whose behalf they act) becomes the default Exchange Provider for that PPN — capturing the ongoing Exchange Provider share of all settlement activity flowing through the PPNs they originated. Individual Engagement Providers can delegate operation of Exchange Provider services to platform providers (e.g. Google, Microsoft, Amazon, Meta, Yahoo, TikTok, Oracle, etc.) that can reuse their existing infrastructure and services at zero marginal cost.

Engagement Providers earn Quantum Privacy Rewards through Evangelized Mode — attribution-tracked distribution of awareness and participation content (EasyAccess Links, vendor portals, social media posts, influencer content, government announcements), with the

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Engagement Provider earning Cascade Premium and Publicity Premium-weighted Quantum Privacy Rewards proportional to the downstream settlement generated by their distribution. EasyAccess Reward Tokens (EARTs) incentivize viral adoption of EasyAccess links, messaging, and opt-ins, serving as loyalty-style rewards that can optionally be converted into Exchange Tokens.

Like Solution Providers, Engagement Providers can be implemented as specialized Exchange Networks or Resource Pools, with their governance terms defining engagement strategies, distribution channels, reward structures, and attribution mechanics. A celebrity or creator may act as an Engagement Provider through their social media presence and viral content, while simultaneously participating as an Exchange Provider or Solution Provider for fan interactions — delegating the operation of those roles to specialized partners in exchange for a share of the resulting revenue, while leveraging their trusted brand and maintaining control of the relationship.

Engagement Providers are the grassroots engine of the Race to Empower (Section 3.7): they create the demand-side forcing functions on incumbents — consumer preference for QPN-routed channels, driven by financial incentives, value alignment, and cultural engagement — that are complementary to but independent of the enterprise adoption cascade.

Architectural Note: Role Composition and Delegation

Any participant can simultaneously serve in any combination of the five roles described above. A healthcare system might serve as a Resource Provider (contributing clinical data), an Exchange Provider (operating Privacy Network infrastructure for its patient population), an Exchange Network operator (combining clinical, claims, and genomic data into value-added Resource Derivatives), a Solution Provider (offering personalized health services to patients), and an Engagement Provider (driving EasyAccess enrollment and engagement through its patient portal, clinician messaging, and billing communications) — earning Exchange Tokens through every role simultaneously.

Any role can be delegated to specialized partners. An individual who acquires Exchange Provider rights through an EasyAccess opt-in can delegate the technical implementation to a specialized vendor while retaining a share of the Exchange Fees. An enterprise that lacks the capabilities to operate its own Exchange Network can contract with an Exchange Network operator while retaining Resource Provider rights to the data, processes, contractual rights, or user populations it contributes. This delegation model enables universal participation regardless of technical capability — the architecture ensures that every participant can earn proportional returns from the value they create, whether they implement the capabilities themselves or delegate to others.

Solution Providers and Engagement Providers, in particular, can be implemented as specialized types of Exchange Networks and Resource Pools — with the Exchange Network or Resource Pool's governance terms defining the customer-facing, pricing, distribution, or engagement mechanics specific to the Solution or Engagement function. This means that the five roles are not rigidly separated categories but composable functions that participants combine and specialize based on their capabilities, strategic priorities, and competitive positioning.

4.6 Ownership, Token Economics & Settlement Mechanics

Accelerators pool resources — contributed through the Quantum Privacy Catalyst Network or direct investment — and use them to develop Exchange Networks, Resource Pools, QP Resources, and Solutions. The Accelerator holds the Quantum Privacy Tokens that represent

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

the ownership and economic rights to these assets. Accelerators may also contract with other Accelerators via shared Resource Pools and common Trust Authorities and Trust Taxonomies, amplifying value generation and Monetization Uplift Multiples for all participating Accelerators without diluting ownership rights or losing domain focus — enabling healthcare, financial services, and sustainability Accelerators, for example, to share cross-domain Resources while each maintains its specialized depth and competitive advantage.

EP3 Accelerators reserve 20% of their Accelerator Tokens for an Incentive & Investment Pool, which is allocated as Quantum Privacy Rewards for Catalyst Network contributions or as returns on Accelerator investments from strategic investors, institutional investors, or grassroots crowdfunding via SAFE Notes or other conventional instruments. The remaining 80% of Accelerator Tokens are allocated to the Accelerator's Participant Pool, distributed as Exchange Tokens earned through ongoing operational participation.

The allocation of Accelerator Tokens for contributions via the Catalyst Network will be governed by AI-assisted allocation models configured by each Accelerator's management or governance, applying formulas and weightings informed by the UTM Premiums and tailored to the Accelerator's domain, strategic priorities, and stage of development. Accelerators will compete to attract participation based on the allocation models they offer — creating market discipline that rewards fair, transparent, and effective allocation and penalizes extractive or opaque approaches.

In addition to graph-based attribution — where each contributor's share is determined automatically by classification, timing, scarcity, and downstream impact without requiring any explicit agreement — Accelerator Managers and participants may publish structured Contribution Bounties: explicit requests for specific contributions with pre-negotiated Quantum Privacy Rewards sharing terms. Bounties accelerate contribution in priority areas and enable collaborative fulfillment when no single contributor can deliver the full scope.

Each bounty specifies a target contribution category, impact estimate, Accelerator context, applicable Launch and Governance Premiums, cascade sharing terms, eligibility requirements, expiration, and visibility level. Bounty reward terms define how the participants' combined share is divided among them—not the absolute amount, which depends on the graph's total downstream impact. Negotiated terms operate within the Quantum Privacy Rewards framework, ensuring compatibility with the Proportionality Premium.

Manager-posted bounties reflect strategic Accelerator priorities; participant-posted bounties enable collaborative fulfillment when a contributor identifies an opportunity they cannot pursue alone. See Section 9.8 for the detailed mechanics of automatic attribution vs. negotiated bounty terms.

Accelerator Tokens — whether allocated based on Catalyst Network contributions or through Accelerator investments — in turn hold pro-rata rights to the Exchange Network Tokens, Resource Pool Tokens, and Resource Tokens associated with the Exchange Networks, Resource Pools, and Resources developed by the Accelerator, along with the stream of Exchange Tokens generated by their participation in PNX settlement activity.

Quantum Privacy Rewards allocations can take the form of Accelerator Tokens, Exchange Network Tokens, Resource Pool Tokens, or Resource Tokens — each of which represents fractional economic rights that ultimately generate a stream of Exchange Tokens as the underlying Accelerator, Exchange Network, Resource Pool, or Resource participates in PNX settlement activity. The eight defined token types in the QPN architecture are:

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Exchange Tokens (EXCH)** — the primary settlement currency, representing fractional rights to revenue and value-added derivatives from the reuse of Resources within the Privacy Network Exchange. Exchange Tokens are generated deterministically when QP Resources are utilized through authorized cross-party reuse and cannot be bypassed within compliant operation.
- **Resource Tokens (RT)** — asset-backed property rights representing ownership, provenance, or usage rights for specific Resources (data, compute, content, contracts, IP rights, or any other tokenized asset). RTs generate Exchange Tokens when their associated Resources are utilized.
- **Resource Pool Tokens (RPT)** — pro-rata ownership or participation rights in a Resource Pool, entitling holders to fractional rights to revenues generated by the use of the pool's Resources. RPTs enable diversification, standardized access, and liquidity across heterogeneous Resources.
- **Exchange Network Tokens (ENT)** — governance and distribution tokens for specific Exchange Networks, entitling holders to a share of the Exchange Tokens generated by settlement activity within that Exchange Network. ENTs capture the compounding asset value of the Exchange Network's Resource Pool ecosystem.
- **Accelerator Tokens (AT)** — distribution rights tied to a specific Accelerator, entitling holders to pro-rata rights to the ENTs, RPTs, and RTs developed by the Accelerator and the stream of Exchange Tokens generated by their participation in PNX settlement. ATs are allocated through the Incentive & Investment Pool (20%) and are not sold directly as fundraising contracts — investments are made into the Accelerator entities themselves.
- **Exchange Root Tokens (ERT)** — perpetual economic claims on 7.5% of all PNX-settled value. The Exchange Root represents the global Exchange Network that spans all Personal and Enterprise Privacy Networks, the Privacy Network Exchange itself, and every individual Exchange Network and Resource Pool within it — making ERTs a participation interest in the aggregate settlement activity of the entire QPN ecosystem. ERTs carry economic rights only — no governance or voting power.
- **EasyAccess Reward Tokens (EART)** — utility and loyalty rewards that incentivize viral adoption of EasyAccess links, messaging, and opt-ins. EARTs function as engagement rewards that can be converted — via the Quantum Privacy Liquidity Pool and mediated through Exchange Tokens — into personalized services, digital content, fiat currency, credit, or any other assets or resource rights available through the Privacy Network Exchange, creating immediate tangible value for participants from the moment they engage.
- **Privacy Network Tokens (PNT)** — hybrid property rights representing ownership or governance participation in specific Privacy Networks. PNTs pool the economic rights that a Personal or Enterprise Privacy Network accumulates through its interactions across the ecosystem — including Quantum Privacy Rewards earned through participation in disparate Exchange Networks and Resource Pools, rights to Resource Tokens published by or derived from the Privacy Network owner's online activities, and rights to Resource Derivatives generated from the Privacy Network's contributed data, engagement, or contractual assets. PNTs enable the Privacy Network itself to function as a portfolio of aggregated economic interests, giving individuals and enterprises a single, portable representation of the total value their Privacy Network has generated and accumulated across the entire QPN.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Accelerator investment decisions for EP3 Accelerators are made by each Accelerator's management, subject to review and approval by Quantum Privacy LLC Managers, who have a right of first refusal to participate in such financings via the Quantum Privacy Investment Network. Accelerator investors receive rights to an allocation of Accelerator Tokens from the Accelerator Incentive & Investment Pool, thereby diluting the amount of Accelerator Tokens available for distribution as Quantum Privacy Rewards via the Catalyst Network.

Any individual, enterprise, or governmental entity can serve as a Resource Provider, Exchange Provider, or Solution Provider via their Privacy Networks, and the rights to Exchange Tokens derived from any of those roles can be allocated to other participants based on terms embedded in Trust Blocks.

4.7 Exchange Root & Public Benefit Allocation

7.5% of all Exchange Tokens generated from PNX settlement activity are allocated to the Exchange Root in perpetuity. This allocation is a protocol-defined structural invariant, deducted from each settlement event before any distribution to Resource Providers, Exchange Providers, or Accelerator pools. Exchange Root Tokens (ERTs) represent the perpetual economic claim on this 7.5% share. These interests will be held by the EP3 Network and allocated to the founders and investors of EP3 Network and WebShield. ERTs confer economic participation only and do not provide governance or voting authority.

The Exchange Root allocation funds both the ongoing development and maintenance of the QPN/PNX core protocol and the EP3 Nature & Humanity Trust. At least 70% of Exchange Root proceeds — expected to grow to over 90% based on stated founder commitments and investor preferences — are allocated to the EP3 Nature & Humanity Trust after the first $1 trillion of cumulative Exchange Root allocations.

The Trust's investment mandate is structurally aligned with the Governance Premium dimensions:

- **Ecological restoration and climate adaptation** (Nature Premium)
- **Education and workforce development** (Humanity Premium)
- **Scientific/medical research & development** (Safety, Humanity, & Innovation Premiums)
- **Digital public infrastructure and civic resilience** (Freedom Premium)
- **Ethical governance innovation** (Ethics Premium)

Unlike traditional philanthropy, the Trust does not spend down principal; it reinvests through PNX market mechanisms — compounding returns through zero-marginal-cost reuse while directing capital toward the governance dimensions the ecosystem is architecturally designed to reward. The Governance Premiums and the Trust form a reinforcing loop: the Premiums create sustained market demand for resources aligned with nature, humanity, safety, freedom, and innovation, while the Trust concentrates long-term capital investment into those same dimensions — ensuring that the economic signals embedded in governance DNA are backed by sustained, compounding institutional commitment. This creates an incentive for investments and contributions aligned with the Trust's mandate immediately, even before the Trust begins receiving allocations from the Exchange Root — because the Governance Premiums guarantee that resources directed toward these dimensions will attract preferential matching, stronger Exchange Token flows, and higher Quantum Privacy Rewards from the moment the first Exchange Networks begin settling.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

The Trust's guaranteed allocation from the Exchange Root ensures consistent and growing demand for resources aligned with its mission — creating immediate incentives to invest in nature, humanity, safety, freedom, and innovation, even before the Exchange is operating at scale or the $1T asset threshold has been met. Investors in the EP3 Network, WebShield, and individual Accelerators that make comparable public benefit commitments — dedicating a significant share of their Exchange Root or Accelerator Token proceeds to the Trust or to equivalent public benefit purposes — will receive preferential treatment in investment allocation, Accelerator participation, and ecosystem positioning, reinforcing the alignment between financial returns and societal impact across the entire investor base.

4.8 PNX Settlement Waterfall

When PNX-settled value flows through Exchange Networks and Resource Pools, the resulting economic value is distributed to participants through a protocol-defined revenue waterfall that ensures every settlement event simultaneously compensates contributors, funds public benefit, handles compliance constraints, and recovers infrastructure costs — in a single atomic operation. The waterfall operates within the Settlement Controller (see B.9) and applies identically whether settlement occurs contractually via the interim dual-use PNX platform or via Quantum Privacy Tokens as the on-ledger settlement infrastructure matures.

The protocol-defined revenue distribution is:

- **Exchange Root (7.5%)** — deducted first from all PNX-settled value, allocated in perpetuity to the Exchange Root as described in Section 4.6.
- **Resource Providers (70% of remaining)** — allocated to the providers of the underlying Resources whose utilization triggered the settlement event, proportional to the value contribution of each Resource as specified in the governing Trust Blocks.
- **Exchange Providers (30% of remaining)** — allocated to the Exchange Providers that enabled the Privacy Network infrastructure through which the Resources were published, settled, and governed.

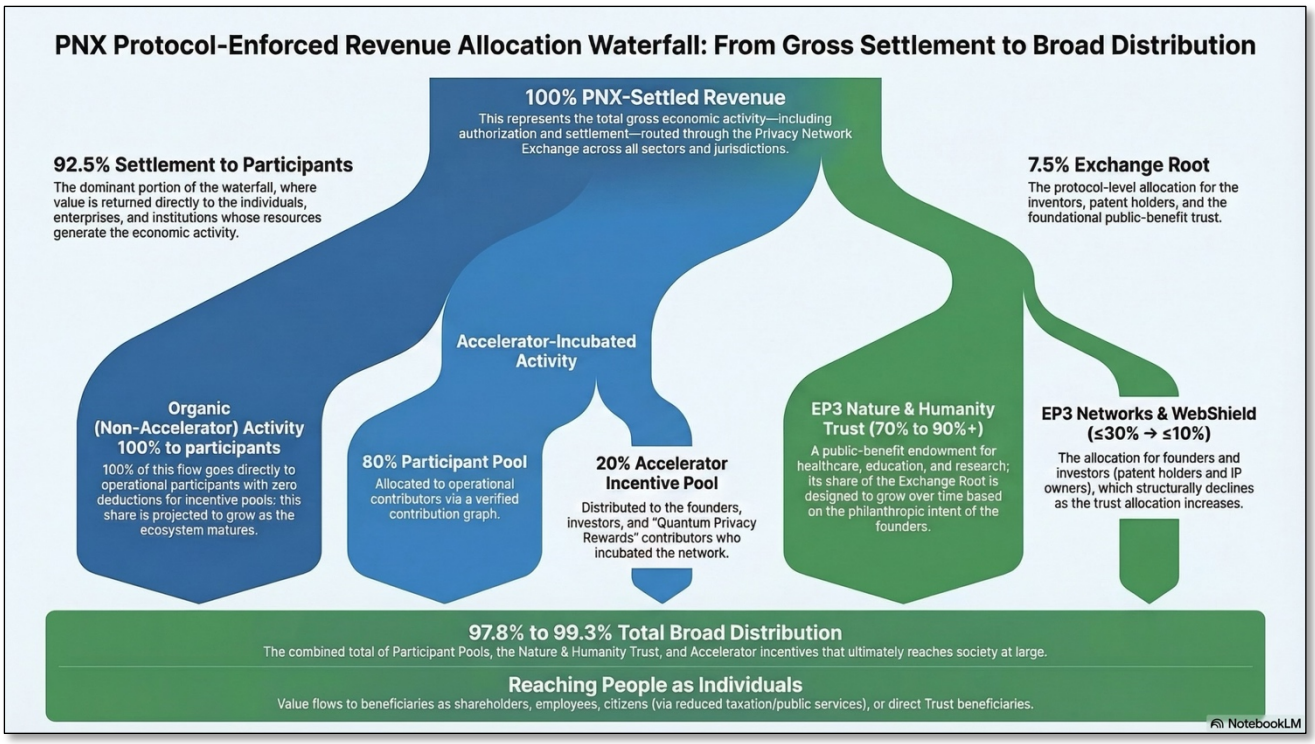
For Accelerator-incubated activity, the combined Resource Provider and Exchange Provider allocations are further split:

- **Participant Pool (80%)** — distributed as Exchange Tokens to participants who earned them through ongoing operational participation, resource contribution, and ecosystem engagement.
- **Incentive & Investment Pool (20%)** — allocated as Accelerator Tokens to Catalyst Network contributors and Accelerator investors, as described in Section 4.5.

For organic (non-Accelerator) activity — settlement flowing through Exchange Networks and Resource Pools that were not incubated by an Accelerator — 100% of the Resource Provider and Exchange Provider allocations flow to the Participant Pool.

Within each pool, individual allocations are determined by the commercial terms embedded in Trust Blocks, weighted by UTM Premiums, Quantum Reputation, and the Attribution Confidence Hierarchy, and enforced through Proof of Trust.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved



Quantum Privacy Rewards Allocation Within the Incentive & Investment Pool

The Quantum Privacy Rewards-specific waterfall within the Accelerator's 20% Incentive & Investment Pool follows a defined sequence:

(1) **Contributor net reward** — the primary distribution to eligible contributors, proportional to their graph-attributed share as computed by the Global Graph Assembly Engine and weighted by UTM Premiums, Quantum Reputation, and the Attribution Confidence Hierarchy.

(2) **Restricted Derivative Rights (RDR) holders** — allocations to contributors whose rewards have been reclassified pending compliance review or redirected to Public-Benefit Derivative Rights (PBDR) pools where prohibited interests are detected. Redirected allocations may flow to the EP3 Nature & Humanity Trust or to other designated public-benefit entities. This ensures that compliance constraints redirect value to public benefit rather than destroy it — settlement continues uninterrupted while affected allocations are resolved.

(3) **Accelerator Operations Fund** — infrastructure cost recovery covering graph resolution compute, compliance service invocations, and settlement processing.

Participants may also voluntarily allocate a portion of their Quantum Privacy Rewards to the EP3 Nature & Humanity Trust or other public-benefit entities. The protocol-defined public benefit allocation from the Exchange Root (Section 4.6) is separate from and additional to any Accelerator-level voluntary or compliance-driven contributions.

A verification fee covering compliance-service and graph-resolution compute costs is deducted from the claimant's gross reward as part of this waterfall, ensuring mathematical solvency — the system processes only claims with sufficient value to cover their own processing costs. Claims that do not meet the minimum threshold are queued for batched processing when the cumulative value is sufficient.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

The broader PNX-level revenue distribution (Exchange Root, Participant Pool, and Incentive Pool splits) is defined in detail in the Settlement Controller (see B.9) and in *Quantum Privacy Network: Universal Access, Exchange, Ownership & AI*.

5. Catalyst Contribution Categories

All Catalyst Contributions are evaluated against the Catalyst Contribution Taxonomy — a canonical, publicly hosted reference document governing AI-assisted classification. The taxonomy uses causal-enablement logic, not keyword matching: the AI evaluates whether a contribution meaningfully enabled, advanced, or created the conditions for ecosystem formation.

5.1 Classification Logic

Classification is causal-enablement-based. The AI assesses:

- Does this work product introduce, connect, or provide access to a decision-maker who could activate or advance an Accelerator?
- Does this work product validate, implement, extend, or accredit a QPN/PNX-compatible capability?
- Does this work product establish governance, compliance, trust infrastructure, or regulatory enablement?
- Does this work product enable, orchestrate, or facilitate multi-party coordination relevant to Exchange Network or Resource Pool formation?
- Does this work product create a reusable component that could be adopted outside the contributor's immediate context?
- Does this work product broker, negotiate, or help establish commercial terms between QPN/PNX participants — such as Resource Provider agreements, Exchange Network operating terms, Trust Block commercial conditions, or value-sharing arrangements — that enable or accelerate Exchange Token settlement?
- Does this work product recruit, close, or onboard a paying customer or end-user for a QPN/PNX-enabled solution, service, or application — directly generating or materially advancing Exchange Token settlement activity?

Classification output includes: primary categories from the taxonomy, cascade indicator (whether the contribution creates downstream activation potential), impact estimate (High/Medium/Low/Uncertain), reusability flag, confidence score (0.0–1.0), and the evaluation model and timestamp.

5.2 The EP3 Contribution Context (Canonical Reference)

The EP3 Contribution Context is a structured, publicly hosted reference document (JSON or structured markdown) that provides the canonical evaluation logic for AI-assisted contribution classification. It serves as the single source of truth that all AI platforms reference, ensuring consistent classification regardless of tool choice.

Contents: the canonical contribution taxonomy (all categories below); classification criteria with causal-enablement indicators and cascade-linkage heuristics; the person and organization identity schemas; active Accelerator context tags; and a versioned changelog.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Hosting: Published at a public EP3 endpoint (e.g., https://ep3.foundation/catalyst/context.json). AI add-ins, extensions, and SuperPrompts reference this URL. The context is cacheable and version-pinned for offline capability.

Governance: Updates are governed by the EP3 Foundation in collaboration with Shared Accelerator governance. New categories may be added; existing categories are never removed — only deprecated and mapped to successors. This ensures that all historical contribution records remain classifiable under the taxonomy version active at the time of contribution.

5.3 Identity & Authentication

Identity Provider: The system utilizes the EasyAccess Authorization Network (OpenID Connect / OAuth 2.0 compliant). The contributor authenticates via one or more verified authentication coordinates — such as email address, phone number, passkey, or platform-native credential — that are bound to their Quantum Privacy Cell (QPC) through the EasyAccess credential graph.

Authentication generates a session token that authorizes the Catalyst to “witness” activity in the target tool. No separate login is required — the contributor’s existing EasyAccess credential serves as their identity anchor across all Catalyst modules.

The QPC serves as the governance and attribution anchor; authentication coordinates serve as the access mechanism. Multiple authentication coordinates may be bound to a single QPC, providing resilience across devices, platforms, and credential changes.

5.4 Eight Primary Categories

Every contribution to the QPN ecosystem — regardless of which Capture Tool recorded it or which Accelerator it belongs to — is classified into one of eight primary categories using the AI Evaluation Pipeline's causal-enablement logic. These categories are not self-reported labels; they are AI-assigned classifications based on what the contribution enabled in the ecosystem formation process. A single contribution may qualify under multiple categories; the AI Evaluation Pipeline assigns the primary category with the highest confidence score and flags secondary categories for review.

Category	Description	Applicable Premiums
Executive Access & Introduction	Introducing C-suite decision-makers to QPN/PNX opportunities; facilitating high-value relationship formation between Accelerator leadership and target enterprise decision-makers.	**Strategic + Timing + Cascade**
Internal Advocacy & Facilitation	Building internal support within enterprises for QPN adoption — executive briefings, champion development, assessment memos, pilot authorization requests, budget sponsorship.	**Strategic + Timing**
Technical & Compliance Validation	Validating QPN/PNX architectural, regulatory, or security requirements; authoring Trust Criteria sets; creating machine-verifiable governance rules.	**Value + Ethics**
Pilot Implementation & Accreditation	Deploying working pilots within enterprise environments; achieving Proof of Trust	**Value + Cascade**

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

	Accreditation for adapters or components; activating operational settlement.	
Ecosystem Orchestration	Facilitating multi-party coordination — connecting participants, enabling joint ventures, structuring Resource Pool or Exchange Network agreements, brokering commercial terms.	**Strategic + Cascade**
Operational Activation & Deployment	Deploying adapters and components into production; connecting data sources; generating Exchange Token settlement; onboarding paying customers or end-users.	**Value + Timing**
Governance & Trust Infrastructure	Authoring Trust Criteria; creating cross-jurisdictional semantic mappings; contributing to UTM ontology; establishing governance frameworks adopted across Accelerators.	**Ethics + Reputation**
Reusable Infrastructure & Application Development	Building components, adapters, or applications reused across multiple Accelerators; creating open adapter specifications; developing integration documentation.	**Value + Cascade**

5.5 Program Structure: Accelerator → Program → Objectives Hierarchy

Contributions are organized within a three-level hierarchy that governs how contributors tag their work, how Managers track progress, and how the Nearby Opportunities feed surfaces relevant objectives.

Level	Definition	Example	Managed By
Accelerator	The top-level organizational container. Corresponds to a specific domain or sponsor entity operating under EP3 governance. Contributors select their Accelerator(s) during onboarding.	Lōkahi Healthcare Accelerator; Quantum Privacy & AI Accelerator; EP3 Network Accelerator	EP3 Foundation / Accelerator Sponsors
Program	A contributor-facing strategy and execution domain within an Accelerator. Contributors select a Program when recording each contribution, tagging it to the strategic context it supports. A single Accelerator may contain multiple Programs with different visibility settings and objective sets.	Lokahi Healthcare (payer focus, contributor-visible); Lokahi Payer Engagement (internal, not contributor-visible); General QPN (cross-accelerator catch-all)	Accelerator Managers
Objective	A specific, measurable goal within a Program with a priority level (Essential / High Value), a target date, a defined goal state (e.g., "2/2 Distinct payer partnerships"), and a status (complete / not started / in progress). Contributions are linked to Objectives by contributors or Managers through the Objective Linking interface.	"Sign 2 payer partnerships with distinct organizations — Q2 2026 — Essential"; "Secure pilot commitment from a health system — Q3 2026 — High Value"	Accelerator Managers

A special Program exists in every Accelerator called "Not sure yet" (or equivalent), with Contributor Visible set to Yes. This is a catch-all bucket for early contributors who are recording their first contributions but are not yet certain which Program they belong to.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Records in this Program are visible to Accelerator Managers for reclassification and objective linking. This eliminates contribution drop-off at the "which program do I belong to?" question during onboarding.

Admin Program Management

Accelerator Managers access a dedicated Admin portal (QPN Catalyst Admin) with four navigation sections: Analytics, Programs, Accelerators, and Organizations. The Programs view displays all Programs within the Manager's Accelerator(s), showing: Program name, parent Accelerator, status (Active/Inactive), number of active Objectives, and Contributor Visibility setting. Clicking into a Program reveals the full Objectives table and the Objective Linking interface, where Managers can link individual contribution records to objectives, update confidence levels (Verified / Strong / Building / Linked), and adjust objective status.

5.6 The Contribution Type Taxonomy: UX Tier Structure

The EP3 Contribution Categories (§5.4) define the semantic classification space. The contributor-facing app exposes this taxonomy through a two-tier UX structure that maps abstract categories to named contribution types with associated XP values:

Engagement Tier

Engagement-tier contributions represent individual relationship or advocacy actions. They are the atomic building blocks of cascade chains — an Introduction leads to a Meeting leads to a Positive Response leads to a Presentation leads to a Partnership Strategy. Each Engagement-tier contribution type has a defined base XP value:

Contribution Type	Description	Base XP
Introduction	Facilitated a first-time introduction between a contact and the QPN/Accelerator ecosystem.	+10 XP
Amplification	Shared, promoted, or amplified QPN/Accelerator content or messaging to a relevant audience.	+15 XP
Positive Response	Received a positive engagement signal (reply, expression of interest, meeting acceptance) from an outreach effort.	+20 XP
Meeting	Scheduled or conducted a substantive meeting with a relevant contact or organization.	+25 XP
Referral	Referred a contact or organization to another contributor or resource within the ecosystem.	+30 XP
Presentation	Delivered a presentation, demo, or briefing about QPN/Accelerator capabilities to a relevant audience.	+35 XP
Partnership Strategy Defined	Developed or documented a partnership approach, engagement strategy, or integration pathway.	+40 XP
Advocacy	Engaged in sustained advocacy (public, governmental, or organizational) on behalf of QPN/PNX.	+20 XP

Major Milestones Tier

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Major Milestone contributions represent outcomes — the conversion of Engagement-tier activity into verifiable, high-value ecosystem commitments. They carry significantly higher base XP and map to the highest-weighted Launch Premium categories:

Contribution Type	Description	Base XP
EP3 Fellow / Affiliate Joins	A new EP3 Fellow or Affiliate organization formally joins the ecosystem.	+100 XP
Strategic Partnering MOU Signed	A strategic Memorandum of Understanding is executed with a partner organization.	+150 XP
Privacy Network Enabled	A new node or privacy domain is enabled on the network.	+200 XP
Partnering Agreement Signed	A formal partnering or distribution agreement is executed.	+200 XP
Accelerator Participation Confirmed	An organization formally commits to participating in an Accelerator program.	+250 XP
Enterprise Customer Added	An enterprise customer is onboarded as an active QPN/PNX participant.	+300 XP
Financing Term Sheet / Investment	A financing term sheet or investment commitment is executed.	+500 XP

The two-tier structure serves a pedagogical function in addition to its classification role: new contributors unfamiliar with the EP3 taxonomy can immediately recognize their recent activity in the Engagement tier, record it, and begin accumulating XP — with Major Milestones serving as visible, aspirational targets for more advanced ecosystem participation. The AI Evaluation Pipeline classification stage maps each Engagement and Major Milestone type to the appropriate EP3 Category automatically, so contributors never need to navigate the full taxonomy directly.

6. Cold-Start Architecture: Operating Before Prerequisites Exist

The conventional wisdom about network platforms of this kind holds that meaningful operation requires a sequence of prerequisites: live token infrastructure before settlement can begin; enterprise-to-enterprise agreement before federation generates value; host trust before data can be shared; certification before components can be deployed; immediate economic transfer before contributions are worth recording; and regulatory clarity before rewards are real. Under the QPN/PNX architecture, every one of these assumptions is wrong.

This section documents the seven architectural mechanisms that collectively enable the network to operate, generate value, and accumulate attribution from day one — before token infrastructure is live, before enterprises have negotiated with each other, before any component has been certified, and before regulatory frameworks have resolved. Each mechanism addresses a different conventional blocker; together they constitute a cold-start architecture with no structural dependency on prerequisites that don't yet exist.

Key Principle: Settlement Is Possible Day One

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Participating individuals and enterprises can enter legally binding Inter-QPC agreements that create enforceable economic relationships immediately, independent of any ledger infrastructure. The QPN/PNX can be self-funding from day one.

6.1 Inter-QPC Agreements

Inter-QPC agreements are standard commercial contracts — executed between individual participants, Accelerators, and/or the Quantum Privacy LLC Managers (EP3 Networks, WebShield) — that specify: resource commitments and commercial terms; target deliverables and milestones; funding contributions (upfront, ongoing, or contingent); participation rights; and how performance against contractual obligations translates into rights to Accelerator Tokens, Exchange Root Tokens, Resource Tokens, and other economic instruments.

These agreements are enforceable in any commercial jurisdiction through conventional contract law, requiring no token infrastructure, no regulatory clarity on token classification, and no ledger activation. Settlement occurs contractually — through standard invoicing, escrow, revenue-sharing, or other commercial mechanisms familiar to every enterprise and law firm on earth.

The practical consequence is transformative: the QPN/PNX can be self-funding from day one. Accelerator anchor participants can make binding investment commitments. Contributors can earn contractually guaranteed rights to future token allocations. Enterprises can commit resources and establish commercial terms for Exchange Network participation. Sovereign entities can structure public-benefit participation agreements. All of this occurs through conventional commercial mechanisms that require no novel legal frameworks, no regulatory pre-approval, and no technology that does not already exist. On-ledger settlement activation becomes a milestone that enhances the system's efficiency and global scalability — not a gate that must be cleared before economic activity begins.

6.2 Migration to On-Ledger Settlement

When Quantum Privacy Token Platforms are accredited and production-ready, contractual interim settlements migrate to on-ledger settlement — converting conventional contractual obligations into cryptographically enforced, automatically settled, globally liquid token flows. This migration is a non-disruptive infrastructure upgrade that improves efficiency, transparency, and automation — not a value-activation event.

The economic relationships, contribution records, and participation rights established during the contractual interim period carry forward with full attribution integrity, because the same deterministic contribution hashing, time-stamped allocation recording, and versioned allocation logic that govern on-ledger settlement also govern the contractual interim. The only difference is the enforcement substrate.

6.3 Person-Centered Aggregation: Bypassing Cross-Enterprise Friction

Under the person-centered aggregation model, cross-host protocol standardization is not a prerequisite for value creation. Aggregation occurs at the level of individual authorization through Personal Privacy Networks and Quantum Privacy Cells, eliminating the need for enterprise-to-enterprise negotiation prior to settlement. Inter-domain protocol harmonization remains an optimization layer for efficiency and federation scale, but it does not gate early-stage economic ignition.

The conventional assumption that cross-host protocol standardization would be a gate rests on a legacy framing that does not apply to the QPN/PNX architecture. In traditional multi-

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

domain systems, when multiple hosts operate independent Privacy Domains, seamless cross-host settlement requires those hosts and their enterprise participants to negotiate inter-domain protocol standards, agree on consistent commercial terms, and reconcile competing allocation models. The QPN/PNX bypasses this entirely, because resources can always flow through and be aggregated in person-centered Resource Pools and Exchange Networks via Personal Privacy Networks and Quantum Privacy Cells.

The mechanism operates through a shared control model that eliminates the need for both enterprise-to-enterprise and enterprise-to-individual negotiation. When an enterprise voluntarily makes data available to an individual — whether through an existing PPN or by creating a new PPN on the individual's behalf — the source enterprise specifies the Trust Credentials and commercial terms bound into the specific Trust Block governing that resource. The individual can choose whether or not to utilize the resource, but in doing so accepts the terms specified by the source enterprise — eliminating the need for case-by-case negotiation between enterprises and individuals, which would be unwieldy or infeasible at population scale. However, since any interaction with a particular individual's data always occurs through their PPNs, the individual retains veto power over anything involving their privacy: they control their own Trust Criteria, they control any sharing of their data outside of Quantum Privacy Cells, and they can specify global Trust Criteria that apply across all of their PPNs. A single person can maintain an unlimited number of separate PPNs, each authorized by a separate opt-in, each with different commercial terms, and the individual can use any combination of PPNs in different contexts based on whatever terms are most favorable in that context. Alternatively, where enterprises do not voluntarily offer resources, Exchange Providers can independently enforce individuals' existing legal, regulatory, and contractual rights to their data — in which case the individual or Exchange Provider sets the Trust Credentials and commercial terms, and the enterprise that originally held the data has no control over the terms under which it is made available. This dual pathway — voluntary enterprise participation with enterprise-set terms, or rights-enforced individual access with individual-set terms — creates the competitive pressure for enterprises to participate proactively on favorable terms rather than have their data made available without their input.

When these person-centered resources are published to Exchange Networks or aggregated into Resource Pools, the enterprise-to-enterprise negotiation problem that plagues conventional cross-domain systems simply does not arise. A healthcare record provided by Hospital A under Hospital A's Trust Block terms and a financial record provided by Bank B under Bank B's Trust Block terms, both flowing through the same individual's PPNs, can be combined in a person-centered Resource Pool without Hospital A and Bank B ever needing to negotiate with each other, agree on data-sharing terms, or even know about each other's participation. Each enterprise's commercial terms are honored independently through the Trust Block architecture; the individual's privacy preferences are enforced through their PPN Trust Criteria; and the resulting aggregated resource is worth far more than either siloed component — generating settlement value that flows back to Hospital A, Bank B, and the individual in proportion to their respective contributions.

This creates a powerful economic dynamic that accelerates rather than impedes cross-host federation. Highly reusable resources aggregated in a common, person-centered Resource Pool are worth far more than the same underlying resources siloed within individual enterprises — because aggregated resources can be combined, recombined, and reused across unlimited Exchange Networks, generating settlement value with each interaction. This value differential creates both a race and an incentive: enterprises that voluntarily empower individuals with control of their resources — by publishing them to Exchange Networks and

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Resource Pools through PPNs — capture a share of the dramatically higher settlement value that aggregation enables. Enterprises that resist find that Exchange Providers and the individuals themselves can achieve the same result by automatically enforcing individuals' existing legal, regulatory, and contractual rights to their own data, as described in the data rights enforcement section above.

The net effect is that cross-host interoperability — traditionally one of the most friction-laden challenges in multi-organizational systems — is resolved not by requiring enterprises to agree with each other, but by empowering individuals to aggregate their own resources across enterprises. The "greedy method" friction of legacy contracts, incompatible technology stacks, and historical practices that slows enterprise-to-enterprise integration simply does not apply when resources flow through person-centered channels. Inter-domain protocol standardization between hosts remains valuable for optimization and efficiency, but it is not a prerequisite for cross-host value creation — making it an enhancement that can proceed incrementally rather than a gate that must be cleared before federation generates value.

6.4 Layered Encryption: Dual-Key Authorization

Layered encryption is one of the simplest and most powerful Privacy Algorithm patterns in the patent portfolio. The architecture operates on two layers that must both authorize for data to be usable:

- **Source Encryption (Layer 1):** The original data owner (a hospital system, an enterprise, a financial institution) encrypts or tokenizes their data with their own keys before it leaves their environment. They retain absolute cryptographic control — without their authorization, the data is opaque bytes regardless of who else holds it.
- **Exchange Provider Encryption (Layer 2):** The host operating the Privacy Domain (Milliman, a Big 4 firm, a sovereign entity) applies an additional cryptographic layer using their governance infrastructure — Unity Catalog access controls, Entra ID authorization, their own key management. Without the host's authorization, the data is also inaccessible.

This transforms the trust question from "do I trust the host with my data?" to "do I trust that my own encryption works?" The source never surrenders cryptographic control. The host never needs to see raw data to enforce governance. A breach of either party alone reveals nothing.

Layered encryption requires no exotic cryptography — it is implementable with standard enterprise tooling today. It maps naturally to the staged governance model: in Stage 0 (single-host containment), layered encryption is optional because the host's controls are trusted; in Stage 1, sources that want additional assurance apply their own encryption before contributing to the PNX; in Stage 2 (multi-host federation), layered encryption becomes the standard pattern ensuring no single host has unilateral access; in Stage 3, more sophisticated Privacy Algorithms supplement the layered encryption foundation.

6.5 Protected Proliferation: Generating Value Before Certification

The most consequential structural insight in evaluating the QPN's timeline is this: certification is not a gate blocking operation — it is a gate governing the scope of operation. The interim PNX platform anchored on Milliman provides a production-grade trusted environment where thousands of adapters, services, AI models, settlement components, and governance mechanisms can be developed, deployed, and generating economic value inside an already-audited containment boundary — without any component needing independent certification, Proof of Trust accreditation, or formal compliance assessment.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

This is not an optimistic interpretation. It is the explicit design of the interim PNX architecture. The model operates in two stages:

- **Stage 1 — Protected Proliferation Inside Trusted Containment:** Components across all six layers are deployed within Privacy Domains hosted inside Milliman's (or another trusted host's) security perimeter. Components are configured so they cannot communicate outside the domain boundary. They inherit the host's existing SOC 2, HIPAA, financial services, and government compliance controls — including the configurable governance provided by Unity Catalog, Entra ID, and other enterprise governance platforms. No certification prerequisite. Only requirement: a trusted host willing to operate the containment boundary.
- **Stage 2 — Incremental Externalization with Accreditation:** When a component is ready to operate beyond the host's boundary — communicating with external systems, serving external users, or exchanging data with other PNX nodes — it undergoes Proof of Trust accreditation. This accreditation is selective: it applies to specific components, not the system as a whole. Components graduate from containment to independent operation one at a time as they are certified. The rest of the system continues operating and generating value inside containment. Certification proceeds in parallel with production operation, not as a sequential prerequisite.

This two-stage dynamic means that the development velocity estimates in the Component Summary Table — and the cascading adoption timelines — are not constrained by certification throughput. Thousands of adapters can be built, tested, and deployed in production inside trusted containment while the Proof of Trust Accreditation Process validates them for externalization at whatever pace accreditation resources allow. The network generates economic value from Stage 1 onward.

Lazy Certification: Why Parallelization Eliminates the Linear Bottleneck

The containment-first architecture enables lazy certification — a pattern where development and deployment proceed at maximum velocity inside trusted containment, and Proof of Trust accreditation is applied selectively and incrementally to components that need to externalize, rather than as a system-wide prerequisite. This means:

- Multiple competing implementations can be developed in parallel inside containment. The best-performing ones are identified through production use before certification resources are spent.
- Certification resources are allocated to the highest-value externalization targets first.
- Gradual federation of multiple hosts proceeds as each host achieves accreditation. The network is not gated by the slowest-certifying component.
- The linear assumption — that the entire system must be certified before any value flows — is structurally incorrect. Value flows from Stage 1 onward.

6.6 Deferred Activation Architecture

All Contribution Records default to DORMANT. No economic value is transferred, promised, or realized at the time of contribution. Records remain dormant until screened by a Proof-of-Trust Accredited Privacy-Preserving Compliance Service (PPCS) and Financial Crime and Fraud Prevention Service (FCFPS), at which point eligible records are activated for Quantum Privacy Rewards allocation and Exchange Token settlement.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Because the only required outputs of the activation process are Quantum Privacy Rewards and Exchange Tokens delivered to the contributor's QPC — which are not publicly disclosed, do not reveal the details of the underlying contribution to any party, and generate disclosure obligations only to tax authorities upon redemption — there is no inherent reason to destroy contribution records from a privacy, compliance, or reputation standpoint. The privacy architecture ensures that sensitive interactions remain protected regardless of whether the associated rewards are claimed.

Contributors who do not wish to receive economic value from specific contributions may voluntarily redirect associated Quantum Privacy Rewards to a Public Benefit Trust of their choice. The EP3 Nature & Humanity Trust is the default recipient for voluntarily redirected rewards. This preserves the contribution's value to the ecosystem — maintaining graph integrity, cascade attribution, and downstream reward accuracy — while ensuring the contributor bears no economic interest in the outcome.

6.7 Jurisdictional Optionality & Entangled Token Embodiment

Exchange Token liquidity sufficient to make Quantum Privacy Rewards economically meaningful would, in a conventional token architecture, require market-making infrastructure, regulatory clarity on token classification, and cross-jurisdictional compliance before participants could realize economic value from their contributions. The QPN/PNX eliminates this dependency through three complementary mechanisms.

First, contractual interim settlement through Inter-QPC agreements — described in Section 6.1 — ensures that Quantum Privacy Rewards and participation rights are economically meaningful from day one through conventional commercial mechanisms, independent of any token liquidity infrastructure.

Second, the QPN architecture provides jurisdictional optionality as a structural property. Quantum Privacy Tokens are not issued in or bound to any specific jurisdiction — they exist across all jurisdictions simultaneously, with jurisdiction selected only at the moment of conversion into fiat currency, tangible assets, or services outside the QPN. The Privacy Graphs underlying QPT value are decentralized, replicated across jurisdictions and platforms, cryptographically opaque yet independently verifiable through Trust Blocks and Proof of Trust — ensuring that no single jurisdiction or token platform controls the evidentiary basis for token value. Because the QPN/PNX's primary economic contribution is coordination and pooled intelligence — value that emerges from the decentralized network itself rather than from jurisdiction-bound physical assets — the specific jurisdiction for computation, settlement, and value accrual can be chosen at execution time, routed to the most favorable regulatory, tax, and execution environment for each activity. This is not regulatory arbitrage in the conventional sense; it is an architectural property of a genuinely decentralized, globally replicated system whose value is inherently non-jurisdictional.

Third, this resilience is further reinforced by entangled token embodiment — a mechanism by which a single Quantum Privacy Token can be simultaneously embodied across multiple token platforms and jurisdictions, with conversion of any one embodiment cryptographically locking the others to prevent double-counting. No single jurisdiction's regulatory change, and no single Tokenization Service Provider's failure, can impair the holder's economic rights as long as any alternative embodiment remains available.

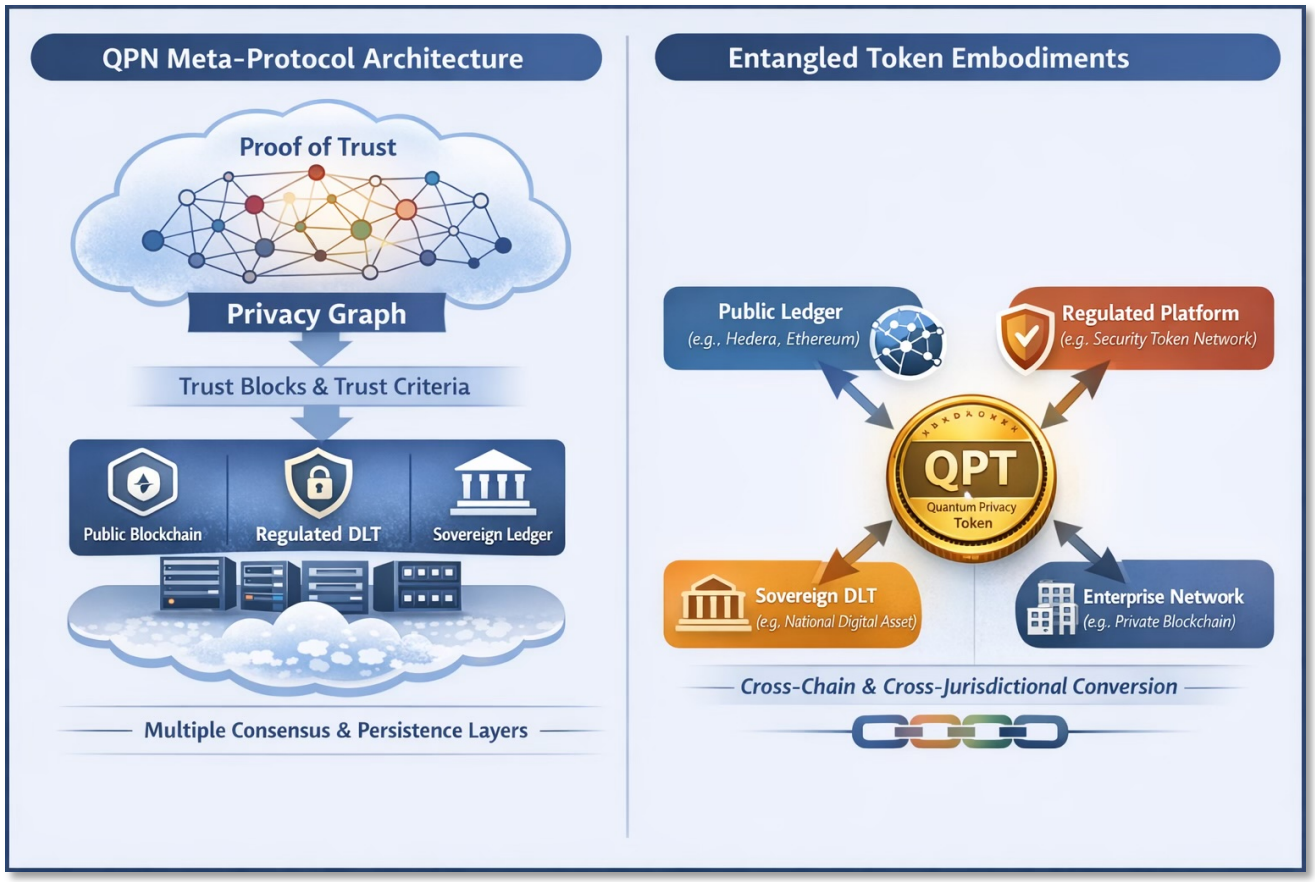
The dual-use settlement architecture — where economic value is generated and tracked from Stage 1 onward, with on-ledger token activation deferred to Track B timing — means that liquidity expansion is an activation-timing question, not an adoption-blocking risk. The

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

custodian-gated fiat boundary model, deferred QPC activation, and multi-jurisdiction tokenization service provider architecture provide additional structural absorbers. Combined with jurisdictional optionality and entangled token embodiment, these mechanisms reduce liquidity expansion from a regulatory gating risk to an optimization task with multiple viable execution paths across dozens of qualifying jurisdictions. The architectural basis for jurisdictional optionality and entangled token embodiment is described in "Jurisdictional Optionality as Architectural Property," a subsection of Section 5.7 of *Quantum Privacy Network — Universal Exchange, Ownership & AI*, as well as in "Execution-Time Jurisdiction Selection" of the *QPT Classifications* document.

6.8 The QPN as a Meta-Protocol for Coordination and Settlement

A key architectural insight underlying the Quantum Privacy Network is that the system is not dependent on any single infrastructure platform, blockchain protocol, cloud provider, or proprietary software stack. Most digital networks are built around a specific technological substrate whose provider effectively defines the boundaries of the ecosystem. The QPN takes a fundamentally different approach: it is designed as a meta-protocol for coordination and settlement that operates above the infrastructure layer rather than within it.



In the QPN model, the canonical record of economic participation is not defined by a blockchain or token platform. Instead, it emerges from the Proof of Trust framework and the Privacy Graph — which record verifiable participation, contribution chains, trust relationships, Quantum Reputations, and settlement events across the network. Trust Blocks encode these events and the Trust Criteria that validate them, and the resulting Privacy Graph becomes the authoritative representation of how value is created, attributed, and governed within the system. Because this trust graph is cryptographically verifiable and independently replicated by participants through their Quantum Privacy Cells, it can be anchored simultaneously on

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

multiple persistence substrates — blockchains, cloud databases, local archives, sovereign data stores, or any combination. The Multi-Substrate Persistence Architecture (see B.6) ensures that contribution records and settlement events survive across decades of technology evolution, device loss, account suspension, and organizational change.

QP Resources exist in a state of quantum superposition across multiple Quantum Privacy Domains simultaneously — each with its own governance context, commercial terms, and authorized purposes — with the specific governance state collapsing to applicable Trust Criteria only upon utilization, enabling simultaneous zero-marginal-cost reuse across any number of Exchange Networks, Resource Pools, and Solution Providers. The architectural properties of superposition, entanglement, and governance inheritance that make this possible are described in detail in *Quantum Privacy Network: Universal Access, Exchange, Ownership & AI*.

Blockchains, token platforms, and settlement infrastructures therefore function as verification anchors and execution environments rather than as the source of truth. This is the same architectural principle that enables jurisdictional optionality and entangled token embodiments (Section 6.7) — applied to infrastructure providers rather than legal jurisdictions.

Infrastructure Optionality and Competitive Discipline

Consensus systems, token services, and persistence layers are treated as interchangeable execution substrates. Multiple providers can operate concurrently, each competing to deliver the most reliable, efficient, and trustworthy service to the network. Hedera Hashgraph is the preferred distributed ledger implementation due to its compliance-oriented architecture, low-latency consensus, and native support for token service primitives — but the architecture explicitly maintains substrate optionality through equivalent implementations on other platforms, including Ethereum, Solana, and cross-chain infrastructure via Axelar, LayerZero, and Wormhole.

If an infrastructure provider becomes technically inferior, economically extractive, or politically compromised, network activity can migrate to alternative substrates without disrupting the underlying trust graph or the economic rights it represents. Because economic rights derive from the Privacy Graph — recorded in Trust Blocks, governed by the Unified Trust Model, and enforced through Proof of Trust — rather than from any specific ledger, no infrastructure provider can capture the system or impose structural dependency. Infrastructure providers, therefore, compete on trustworthiness, performance, cost, and compliance quality rather than on platform lock-in — a competitive dynamic that aligns with the Freedom Premium's guarantee against surveillance and the Sharing Premium's structural preference for openness over proprietary control.

This architecture ensures that the QPN remains resilient even as the underlying technology landscape evolves. Providers that maintain neutrality and reliability are rewarded with greater adoption and routing preference through Quantum Ratings; providers that become extractive or unreliable are replaced through the same competitive selection dynamics that govern every other participant in the ecosystem.

Implications for Network Formation and Adoption

Designing the QPN as a meta-protocol has profound implications for the adoption cascades described in Section 3.9. Traditional platforms must convince participants to migrate into a new ecosystem — a process that creates friction, switching costs, and resistance. The QPN requires no migration. Existing platforms, enterprise systems, cloud environments, AI models,

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

and developer tools connect to the network through dual-use deployment, with their capabilities becoming QP Resources that participate in Exchange Networks and Resource Pools without replacement, reconfiguration, or disruption to existing operations.

This dramatically lowers the barrier to participation and eliminates the cold-start problem that defeats most platform-adoption models. Every enterprise system already operating — every Databricks environment, every Salesforce instance, every EHR platform, every cloud deployment — is a potential QPN participant that can begin generating PNX settlement value through dual-use integration at zero incremental infrastructure cost. The meta-protocol design means that the QPN does not compete with existing infrastructure for adoption; it layers trust, governance, ownership, and settlement onto infrastructure that participants have already deployed and are already operating.

The result is a network formation model in which infrastructure providers, enterprises, sovereign entities, and individual contributors can all participate simultaneously — each through their existing infrastructure, each earning proportional returns through Universal Ownership, and each reinforcing the adoption cascades that drive the system toward global scale.

6.9 Grassroots Cascade: Evangelism, Ownership & Demand

The eight mechanisms above collectively neutralize the conventional prerequisites for enterprise-driven network formation. A ninth mechanism creates an independent, bottom-up path to critical mass that does not depend on enterprise sponsorship at all.

The Grassroots Evangelism-Ownership-Demand Cascade operates through four self-reinforcing stages:

- **Stage 1 — Evangelize and Accumulate.** Individuals learn about the opportunity and begin contributing through Active mode while evangelizing through Evangelized mode. Their QPCs accumulate durable economic rights through Quantum Privacy Rewards. They need no enterprise approval, capital, or institutional sponsorship. The behavioral activation system provides immediate feedback. This stage begins in Phase 0.
- **Stage 2 — Crowdsource Accelerators and Define Demand.** As contributor density reaches critical mass in specific domains, contributors collectively form Accelerators — defining market requirements, specifying Engagement Networks, Exchange Networks, and Resource Pools; and attracting or crowdsourcing funding through the Accelerator Incentive & Investment Pool. The people who will consume the products define what those products should be, with economic ownership of the networks that deliver them.
- **Stage 3 — Preference and Demand Routing.** Once QPN-routed solutions exist, contributors prefer them over incumbent alternatives through ***financial incentive*** (ownership makes QPN-routed consumption rational), ***value alignment*** (Universal Ownership allocates more value to individuals), and ***societal activism*** (routing through QPN accelerates the transition to a more equitable model). These three motivations are individually sufficient and mutually reinforcing.
- **Stage 4 — Incumbent Forcing Function.** When a material fraction of an incumbent's user base prefers QPN-routed alternatives, the incumbent faces a choice that worsens with delay. Universal Access means individuals can exercise their rights through PPNs that operate on the incumbent's own infrastructure or incorporate existing apps, content, and solutions via dual-use deployment. Initially, these Privacy Network-enabled alternatives layer privacy, ownership, and settlement onto the incumbent's existing capabilities. Over

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

time, they evolve to replace them entirely — with person-centered, crowdsourced solutions that are more efficient, offer superior capabilities, and reward participants rather than subjecting them to extractive practices. The QPN's ability to bootstrap new networks by incorporating any existing resource, infrastructure, or solution through dual-use deployment, then incrementally replace them with native systems built through crowdsourced development and funded through Accelerator Incentive Pools, makes resistance existentially risky. The only sustainable strategy is to join the Accelerator Network and participate as a Privacy Network Provider.

The Grassroots Cascade is structurally independent of the Enterprise, Investment, and Sovereign Cascades described in Sections 3.9 and 6.10–6.11. All four cascades operate through distinct mechanisms, distinct participants, and distinct incentive structures. Their combination produces dramatically higher cascade probability than any individual pathway because all four must independently fail for critical mass not to be reached, each validates the others' thesis, and none can be blocked independently without triggering the others. The four-cascade architecture has no single point of suppression.

6.10 Investment Cascade: Competitive Capital & Ecosystem Acceleration

A tenth mechanism can independently fund the development and deployment of the QPN/PNX without requiring enterprise commitments, grassroots critical mass, or sovereign sponsorship.

The Investment Cascade operates through the same competitive dynamics currently driving hundreds of billions in annual AI infrastructure investment. A single credible anchor investor — whether a technology founder, a venture or growth equity firm, a sovereign wealth fund, or a corporate venture arm — providing sufficient capital to independently develop the Quantum Privacy Catalyst Network and Foundational Enabling Services would anchor a Quantum Privacy Investment Network, providing funding through EP3 Networks and various Accelerators. This initial commitment would trigger competitive investment responses from peer investors who cannot afford to let a rival establish foundational positioning in the privacy exchange layer.

The Investment Cascade is structurally independent of the Enterprise and Grassroots Cascades: it can fund development, Accelerator formation, and initial settlement activity without requiring any enterprise to commit as an anchor or any grassroots community to reach critical mass. Capital deployed through the Quantum Privacy Investment Network flows into Accelerator Incentive & Investment Pools via conventional instruments (SAFE Notes, convertible notes, equity), generating Accelerator Token allocations that compound as the ecosystem grows. The capital efficiency is extraordinary — the QPN's direct costs of less than $50M catalyze $10–25B+ in ecosystem investment, with a leverage ratio of 200–500x driven by competitive self-interest among enterprises, vendors, and investors.

The parallel to the current AI investment cascade is direct: AI investors are deploying hundreds of billions at stratospheric valuations, teaming with hyperscalers and AI labs to build out infrastructure with uncertain and distant returns. The QPN investment thesis is structurally superior — dual-use infrastructure means zero incremental build-out cost, settlement revenue begins from day one, and the addressable value is GDP-scale. An investor who recognized the AI infrastructure opportunity early captured extraordinary returns; the QPN opportunity is analogous but operates at larger scale with lower capital requirements and faster economics.

Once the Investment Cascade fires, it accelerates all three other cascades simultaneously: funded Accelerators reduce enterprise participation risk (Enterprise Cascade), funded

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

development produces the tools and infrastructure that grassroots contributors need (Grassroots Cascade), and funded proof-of-concept deployments provide the institutional credibility that sovereigns require (Sovereign Cascade).

6.11 Sovereign Cascade: From One Government to Global Scale

An eleventh mechanism can anchor institutional adoption through government-driven deployment, independently of private-sector enterprise commitments, grassroots participation, or investor funding.

The Sovereign Cascade operates through a single sovereign entity establishing a Sovereign Accelerator to develop the infrastructure and services that any government needs to serve its constituents — healthcare delivery, education, workforce development, public safety, environmental monitoring, citizen services, identity management, and regulatory enforcement. The QPN's architecture is uniquely aligned with sovereign priorities: it preserves governmental authority over data within its jurisdiction, enhances regulatory enforcement capabilities through Proof of Trust and the Unified Trust Model, and creates economic value that flows to citizens through Universal Ownership rather than being extracted by platform intermediaries.

A sovereign commitment triggers adoption through three reinforcing mechanisms. First, direct funding — through government grants, procurement contracts, or sovereign wealth investments — provides capital to develop domain-specific Exchange Networks and Resource Pools tailored to public-sector needs without requiring private investment. Second, government adoption de-risks the opportunity for enterprises, investors, and other sovereigns, because a sovereign anchor provides the regulatory credibility and institutional legitimacy that other participants require before committing at scale. Third, the capabilities developed for one sovereign proliferate to others through shared vendors — the Big 4 professional services firms, hyperscalers, systems integrators, and government technology providers that serve multiple governments simultaneously. When a vendor deploys a QPN-enabled citizen services platform for one government, the same capabilities become immediately available to every other government that vendor serves — creating cross-sovereign cascade dynamics through existing vendor relationships rather than through direct government-to-government coordination.

The State of Hawaii's statewide health transformation initiative — already funded and anchoring the Lokahi Healthcare Accelerator — demonstrates the viability of this pathway. Hawaii provides the proof-of-concept: a production deployment on existing infrastructure, in a regulated domain, with funded institutional commitment. As the Lokahi model demonstrates settlement value, other states, national governments, and international organizations face the same competitive dynamics that drive enterprise adoption — the first sovereign to commit captures governance anchoring and trust taxonomy positioning that later entrants cannot replicate.

The Sovereign Cascade is structurally independent of the other three: a government can fund, develop, and deploy QPN infrastructure through its own authority and budget processes without requiring enterprise anchor commitments, grassroots critical mass, or private investor capital. Once activated, it accelerates all three other cascades — sovereign credibility attracts enterprise participation and investment, while government-deployed services create the population-scale PPN enrollment that drives grassroots adoption.

7. Implementation Summary

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Full implementation specifications for the Foundational Enabling Services are contained in Appendix B.11, and the QPN Catalyst Application and Capture Module specifications are in Appendix B.12.

Foundational implementation architecture, the crowdsourced development strategy, vendor competition model, adoption cascade dynamics, and the Milliman-anchored production environment are described in Appendix A. This section provides the strategic overview of architecture, governance progression, Universal Compliance, the QPN Catalyst reference implementation, and the launch phases that ground the implementation plan.

7.1 Six-Layer Architecture

The Catalyst Modules and Foundational Enabling Services are organized into six architectural layers reflecting dependency relationships. Lower layers are foundational; upper layers rely upon capabilities below. All components across all layers can be developed in parallel, with additional capabilities phased in incrementally as foundational layers mature.

Layer	Components & Role
QPN Catalyst Layer	Catalyst Modules (WebVector, VoiceVector, CodeVector, DocVector, AgentVector, CommVector, MeetVector, MessageVector), AI-Assisted Evaluation, Personal Archive & Contributor Intelligence Module, and Settlement Controller. A minimal implementation — such as the deployed QPN Catalyst application (WebVector) — is sufficient to begin crowdsourcing, attributing, and compensating contributions to all Foundational Enabling Services. Additional Catalyst Modules activate incrementally as the ecosystem matures.
Core Runtime Layer	QPC lifecycle management at population scale, EasyAccess enrollment and adoption infrastructure, Exchange Network and Resource Pool execution engine, and Quantum Rating System for trust signaling. Can operate with delegated governance (Stage 1) before the Governance Layer is fully deployed.
Cryptographic & Identity Layer	Post-quantum cryptographic substrate and privacy-preserving identity resolution infrastructure. Security and identity foundations all other layers depend on for privacy guarantees and cross-domain participant matching.
Resource Publishing Layer	Bridges connecting the PNX to ten major categories of enterprise software — data catalogs, cloud storage, CRM systems, CI/CD pipelines, model registries, EHR systems, financial data, identity graphs, audience graphs, API gateways. Each enables existing enterprise resources to become settleable PNX Resources without migration or duplication.
Governance & Compliance Layer	Unified Trust Model Runtime and Governance Verification Bridge. Not required for initial operation inside trusted containment — becomes essential for multi-host federation.
Exchange, Content & Liquidity Layer	Personalized exchange engine, AI content generation and settlement engine, and Token Platform Bridge. Token Platform is the only explicitly sequenced component (Track B, activated after settlement mechanics are proven).

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Skills as the Universal Extensibility Mechanism. Across the Catalyst architecture, Skills are the universal pattern for adding new capabilities without writing new code. Data Plane Skills add intelligence capabilities — domain-specific extraction vocabularies, detection patterns, nudge generation strategies, evidence matching heuristics, introduction suggestion logic. Control Plane Skills add operational capabilities — command interpretation, approval framing, admin operations. Both use the same definition pattern, both are QPC-scopeable (an accelerator can enable or disable skills per program), and both are independently evaluable. Adding a new accelerator's domain-specific extraction vocabulary, a new contribution detection pattern, or a new admin operation means adding a skill definition — not building custom software. This is the mechanism by which the architecture scales across accelerators without proportional engineering cost, and it is what makes the non-proportional capital scaling claim structurally grounded: each new accelerator inherits the full capability stack and extends it through skill definitions rather than bespoke development.

7.2 Staged Governance: Delegated → Federated → Cryptographic

A critical architectural insight is that the Governance & Compliance Layer is not a prerequisite for initial network operation. Governance follows a three-stage progression that enables the network to generate value immediately while progressively strengthening governance infrastructure.

- **Stage 1 — Delegated Governance (Dual-Use Privacy Domains):** The PNX delegates governance to the host's existing infrastructure. Inside Milliman's trusted containment, Databricks Unity Catalog controls data access with fine-grained column-level security, row filters, and data lineage tracking. Microsoft Entra ID enforces conditional access policies, role-based access control, and cross-tenant collaboration rules. Snowflake's dynamic data masking and row-level security provide additional governed data access. AWS Lake Formation's tag-based access control governs cloud-native resources. Datavant's privacy-preserving entity resolution enables governed cross-dataset linkage without exposing identifiable information. These systems are not primitive placeholders — they represent billions of dollars in enterprise governance investment, already configured, already audited, already trusted by regulators. The PNX operates within this governance from day one.
- **Stage 2 — Federated Governance:** When multiple hosts need to interoperate — Milliman's PNX connecting to a Big 4 firm's PNX, sovereign accelerators coming online, cross-host settlement beginning — the Unified Trust Model Runtime provides a common machine-interpretable language so different hosts can programmatically verify each other's controls. This is the "making implicit explicit" step: taking what Unity Catalog enforces and what Entra ID enforces and expressing both in terms that a counterparty can verify.
- **Stage 3 — Cryptographic Governance:** Once governance is machine-interpretable, it can be cryptographically enforced within Quantum Privacy Domains — offering zero-knowledge proofs that Trust Criteria are satisfied without revealing underlying data, Trust Block attestations anchored on immutable ledgers, and Proof of Trust accreditation continuously monitored rather than point-in-time audited.

The Core Runtime Layer components can operate under Stage 1 delegated governance from day one. The Governance & Compliance Layer components are developed in parallel but are not blocking — they enable federation and scale, not initial operation.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Privacy Domain Tier Progression

The governance stages above map to a three-tier Privacy Domain model, defined in *Quantum Privacy Network — Universal Exchange, Ownership & AI*. Each tier represents a different root of trust underlying the privacy guarantee. All three tiers share identical Trust Block mechanics, settlement interfaces, and economic behavior — the distinction is solely the strength and nature of privacy enforcement.

- **Tier 1 — Dual-Use Privacy Domains:** Enforcement relies on the host's existing governance, compliance infrastructure, and layered multi-enterprise cryptography. This is the operational tier during Stage 1 (Delegated Governance) and the immediate deployment model for Protected Proliferation Inside Trusted Containment. Dual-Use Privacy Domains inherit enterprise-grade security from existing infrastructure without requiring new cryptographic deployment.
- **Tier 2 — Classical Privacy Domains:** Enforcement relies on hardware- or hypervisor-level isolation through attested confidential compute environments (AWS Nitro Enclaves, Azure Confidential Computing, GCP Confidential Space, or equivalent platforms meeting defined Trust Criteria). Neither enterprise administrators nor cloud vendors can independently access data within the enclave. Classical Privacy Domains become available as secure enclave capabilities are integrated during Stage 2 (Federated Governance), enabling Incremental Externalization with Accreditation — where privacy guarantees are rooted in hardware attestation rather than enterprise policy alone.
- **Tier 3 — Quantum Privacy Domains:** Enforcement relies on mathematically provable guarantees through accredited Privacy Algorithm implementations. Quantum Privacy Domains provide the strongest privacy assurance — operations execute on cryptographically protected representations, and correctness can be verified without any party accessing plaintext. This tier becomes available as Stage 3 (Cryptographic Governance) matures.

In addition, hybrid **Semi-Quantum Privacy Domains** can operate with full mathematical guarantees for all operations within their boundary while delegating specific workloads that require plaintext execution to nested Classical Privacy Domains for backward-compatible computation — combining Tier 3 assurance for the overall domain with Tier 2 enclave protection for legacy software compatibility.

Classical Privacy Domains: Backward-Compatible Secure Execution

Classical Privacy Domains serve a dual purpose: they provide the secure-enclave infrastructure for Tier 2 of the trust model, and they accommodate workloads in which software components, analytical engines, AI models, or commercial platforms require plaintext access to data and cannot execute directly on cryptographically protected representations. In this latter role, Classical Privacy Domains can be nested within Quantum Privacy Domains to create the hybrid Semi-Quantum architecture described above.

A Classical Privacy Domain is an attested confidential compute environment instantiated within a trusted execution platform. These environments provide hardware- or hypervisor-enforced isolation, cryptographic attestation of runtime configuration, restricted ingress and egress channels, and protection from operator or host-level visibility.

When a Resource's Trust Criteria specifies plaintext execution requirements, the required input interfaces, schemas, terminologies, and protocol constraints are defined in the Resource Description and Trust Block of the software or algorithmic component. While still within the governing Quantum Privacy Domain, protected inputs are mapped, normalized, and

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

transformed into the required formats and semantic structures specified by those Trust Criteria — without exposing plaintext outside the cryptographic boundary.

Only after this transformation occurs within the Quantum Privacy Domain are the protected inputs routed into an attested Classical Privacy Domain. Where necessary, input adapters operating within the Classical Privacy Domain's confidential execution boundary map between the QPN's internal data representations and the specific semantics, interfaces, and protocols expected by the software component — enabling interoperability with unmodified legacy software without exposing data outside the enclave. Decryption occurs exclusively inside the confidential execution boundary. The software component executes unmodified on plaintext data within that boundary. Where necessary, output adapters then map the component's native outputs back into QPN-compatible representations, and embedded Privacy Agents operating inside the same attested environment enforce the applicable Privacy Algorithm — applying transformation, tokenization, partitioning, aggregation, redaction, obfuscation, noise injection, or other Trust Criteria-specified controls — before any information exits the Classical Privacy Domain.

The Trust Criteria governing each Classical Privacy Domain specify acceptable confidential compute platforms, required attestation proofs, input and output interface constraints, mapping requirements, and egress enforcement rules.

Because Classical Privacy Domains are governed under the same Unified Trust Model as Quantum Privacy Domains, they inherit the same privacy, cybersecurity, regulatory, and contractual enforcement guarantees. This mechanism preserves backward compatibility with existing enterprise software stacks, eliminates the need for structural rewrites, and allows workloads requiring plaintext execution to participate in the Universal Compliance architecture without weakening its boundary protections.

7.3 Universal Compliance: Safe Deployment without Accreditation

Automated Proof of Trust accreditation at scale — where thousands of individual resources, adapters, and components must each be independently assessed and certified — appears at first glance to be a requirement for widespread adoption and a significant throughput constraint. Manual accreditation processes can handle dozens to hundreds of components; scaling to thousands would require automation that is itself a substantial development and administrative task.

However, this framing fundamentally mischaracterizes the compliance architecture of the QPN/PNX, because the Quantum Privacy Domain establishes a cryptographic compliance perimeter within which resource-level accreditation is not required for safe operation — reducing it from a gating prerequisite to a value-enhancing optimization.

The QPN offers a general-purpose Universal Compliance to unlocking regulated, proprietary, or personal data and making it safely available for automation, orchestration, optimization, personalization, and policy enforcement on a global scale — without risking violations of privacy, regulatory compliance, or contractual restrictions of any participant.

This Universal Compliance path operates through three architectural layers:

- **First Layer: Quantum Privacy Domains.** All data is routed through one-way Privacy Algorithms into shared, decentralized Quantum Privacy Domains that support arbitrary computation within a cryptographically enforced boundary without revealing meaningful information outside that boundary to any person, system, or organization. The cryptographic guarantees ensure that no meaningful information can be revealed outside the decentralized boundaries of Quantum Privacy Domains unless explicitly authorized

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

under governing Trust Criteria. While the resulting network of global Privacy Graphs is entangled — enabling cross-domain linking, analytics, and AI — it is subdivided into cryptographically self-contained Quantum Privacy Domains, each of which ensures that no data ingested or generated within it is revealed without first verifying the Trust Criteria of all participants through Proof of Trust. Once within this perimeter, data from any source Privacy Domain can be efficiently linked, transformed, reprocessed, and reconciled into Privacy Graphs optimized to support AI training and inference, analytics, process orchestration, optimization, personalization, policy enforcement, and attribution. The Trust Blocks of any Resource Derivatives generated incorporate links to the Trust Criteria of all of their Resource inputs, ensuring that the Trust Criteria of all upstream Resources are automatically inherited — providing end-to-end enforcement of the privacy, cybersecurity, regulatory compliance, and commercial rights of all participants regardless of how their Resources are combined, reprocessed, or reused.

- **Second Layer: Federated Cryptographic Coordination.** The entanglement across Quantum Privacy Domains described above is not ad hoc — it is governed by a federated cryptographic coordination layer. The one-way Privacy Algorithms ensure that data flows only into Quantum Privacy Domains protected by the same Privacy Algorithms — or by common families of Privacy Algorithms with equivalent or better protection guarantees governed by common Trust Authorities and mapped into common Trust Taxonomies — and that no meaningful data or derivatives can ever be revealed outside their boundaries except under explicitly authorized Trust Criteria. This federated coordination enables the network of entangled Quantum Privacy Domains to frictionlessly distribute computation, share data, and coordinate across organizational and jurisdictional boundaries, all intrinsically protected by the same privacy, cybersecurity, regulatory compliance, and contractual enforcement guarantees that govern each individual domain.
- **Third Layer: EasyAccess Authorization Network.** When data or derivatives must cross a Quantum Privacy Domain boundary to reach an identified person or system — the one case where the cryptographic perimeter is intentionally bridged — the EasyAccess Authorization Network provides privacy-preserving, person-centered cross-organizational authorization and policy enforcement on a global scale. All Privacy Domains — Quantum and Classical — can safely rely on this mechanism because the EasyAccess Authorization Network itself is anchored by a decentralized Quantum Privacy Domain, which can be partitioned into Quantum Privacy Domains operating within participants' Personal or Enterprise Privacy Networks as EasyAccess Sub-Domains. This allows existing enterprise or consumer authorization systems and infrastructure to be seamlessly incorporated into the EasyAccess Authorization Network as dual-use infrastructure within their respective EasyAccess Sub-Domains — allowing existing authorization policies to be enforced based on existing infrastructure and practices as-is (thereby inheriting their existing accreditations and trust) while enhancing their reach and robustness via the crowdsourced, Quantum Privacy and Proof of Trust enabled capabilities. The EasyAccess Authorization Network's underlying Quantum Privacy Domain ensures that the only thing revealed to outside parties is privacy-preserving authorization credentials, which do not reveal what Resources are being accessed or any other potentially sensitive context.

Taken together, this ensures that both existing enterprise policies and all aspects of the Unified Trust Model — privacy, cybersecurity, regulatory compliance, commercial and contractual terms, systems administration, and personal preferences — embedded in the Trust Blocks of any Quantum Privacy Resources can be consistently enforced across all Privacy Domains, without revealing meaningful information outside the protected boundaries.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Eliminating Accreditation as a Scaling Constraint.

Universal Compliance substantially eliminates the need for automated resource-level accreditation as a gating factor for publishing resources and making them available for use within the Quantum Privacy Network and Privacy Network Exchange. Resource-level accreditation is not required for contained operation within accredited Quantum or Classical Privacy Domains, but becomes increasingly valuable as externalization, portability, and selective data revelation increase, and supports more seamless coordination with existing dual-use processes and solutions.

Automating the Proof of Trust Accreditation of individual resources remains valuable because it more thoroughly documents provenance, lineage, structural integrity, governance alignment, and declared Trust Criteria — making resources more semantically meaningful, trustworthy, interoperable, reusable, and therefore more commercially valuable.

In combination with the EasyAccess Authorization Network, Personal Privacy Networks, and their associated QPCs, robust resource-level accreditation enables more personally identifiable, regulated, or proprietary data to be selectively revealed outside protected Privacy Domains under controlled conditions — expanding the range of use cases and increasing settlement value.

In addition, the ability to support global-scale decentralized aggregation, linking, and computation of Resources within a shared Quantum Privacy Domain greatly enhances the efficiency and effectiveness of implementing automated governance, compliance, and accreditation. Within the cryptographic perimeter of a Quantum Privacy Domain, automated assessment systems have comprehensive visibility into every Resource, every Resource Derivative, every Trust Block, and every lineage record — without encountering the access-control fragmentation, privilege-escalation risk, or cross-organizational data-sharing barriers that make comprehensive assessment prohibitively complex in conventional enterprise environments.

Under this model, accreditation is not a prerequisite for contained participation within accredited Quantum or Classical Privacy Domains operating under enforced boundary-level controls. It is a progressively strengthening signal that enhances portability, externalization, liquidity, and commercial value — allowing economic ignition to proceed immediately within accredited Privacy Domains while reputation depth and formal certification sophistication expand in parallel.

Minimum Accreditation Requirement

The only accreditation required to enable the Universal Compliance model is for: the cryptographic layer of the Quantum Privacy Domain — including Privacy Algorithms, Privacy Agents, and boundary enforcement infrastructure; approved Classical Privacy Domain configurations that meet defined Trust Criteria for confidential execution; and the UTM content that specifies the core general-purpose capabilities of the EasyAccess Authorization Network. Privacy Algorithms remain general-purpose and neutral with respect to vendor, schema definition, Trust Criteria, authorization model, and application domain. They can be incrementally updated and enhanced over time through a robust process governed by multiple authorities. This capability can be incubated and deployed at scale on the interim PNX platform during Stage 1 of the rollout, initially operating as Dual-Use Privacy Domains using simple Privacy Algorithms based on delegated governance to Trusted Containment platforms (such as Milliman or a Big 4 auditor) with layered cryptography, and progressively transitioning to Classical Privacy Domains as approved confidential compute environments are integrated and accredited, and/or Quantum Privacy Domains based on accredited Privacy Algorithms.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Enabling Privacy-Preserving or Anonymous Interaction with Quantum Privacy Interaction Hooks (QP Hooks)

When systems running within Quantum Privacy Domains require interaction with people or with external dual-use systems, this is orchestrated via entangled Personal or Enterprise Privacy Networks through their associated Quantum Privacy Cells, using Quantum Privacy Interaction Hooks (QP Hooks) sent between domains. QP Hooks do not reveal meaningful information from shared Quantum Privacy Domains. Instead, the EasyAccess Authorization Network authorizes each Personal or Enterprise Privacy Network to access the tokenized context graph contained in each QP Hook, which in turn pulls the necessary data for implementing the user interaction or computation from the original source Privacy Domains — before the data was ingested into the Quantum Privacy Domain – or from an alternative Privacy Domain that has access to and authorization to use the same or suitably equivalent data.

The EasyAccess Authorization Network can trace the available sources for specific data — down to the attribute level — that must be disclosed to a given person or system to support a process executing within the Quantum Privacy Domain, and identifies one or more sources for each individual data element with authorized access paths – none of which involve disclosing information from the shared Quantum Privacy Domain itself.

Because the same underlying data — a person's name, their employer, the price paid for a purchase, a clinical result — is often stored by multiple systems and controlled by different organizations or individuals with different rights, restrictions, and commercial terms, the Authorization Network can optimize retrieval and minimize friction by selecting the most cost-effective, trustworthy, accessible, and conveniently authorized source for each element. In many cases, this will be the online user's or record subject's Personal Privacy Network, or an Enterprise Privacy Network in which they are already an authorized recipient – but it could be pulled from any Privacy Network or available API.

Importantly, the data graph necessary to orchestrate a particular step of a process can be assembled from a decentralized network of sources, each of which individually holds only fragments of the overall graph. The most sensitive data — clinical records, financial transactions, behavioral patterns — can, in most cases, be analyzed exclusively within Quantum Privacy Domains and need not be revealed to any external party. For example, a Personal Health Network might analyze a complete graph of personal records — food purchase loyalty data, credit card records, clinical data, smart watch sensor readings, and self-reported symptoms — and determine that the individual is at high risk of an acute cardiovascular event. This might trigger recommendations for imaging or genomic testing to enable a more accurate diagnosis and treatment plan, revisions to their diet, a personalized exercise program, and lifestyle changes that reduce stress. To facilitate this, the service might suggest alternative restaurant choices, food purchases, and menu selections; offer personalized discount coupons subsidized by their health insurance or employer; send a link to an exercise app and an invitation to join a neighborhood hiking club, sports league, or gym; and help book transportation to a testing facility — all without revealing any sensitive healthcare information to any of the people, organizations, or systems involved. Neither recipients nor sources have visibility into the broader computational context, preserving privacy and compliance while enabling end-to-end automation and orchestration.

The various resource providers and participants who contributed to enabling this end-to-end process — the data providers who contributed clinical records and loyalty data, the AI models that performed risk analysis and personalization, the computing platforms that hosted Quantum Privacy Domains, the individuals who facilitated introductions or referrals, the insurance plan that subsidized incentives, and the service providers who delivered the

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

outcomes — would each share in the revenue or value created via PNX Settlement, proportional to their contribution, without having visibility into the underlying clinical motivation, the specific resources contributed by others, or the identity of the individual whose health outcome they collectively improved. In addition to PNX-settled value, the process drives incremental dual-use revenue to participating businesses — the restaurants, food stores, gyms, exercise apps, testing facilities, and transportation services each gain a paying customer they would not otherwise have reached, creating economic value that compounds beyond the settlement layer.

Similarly, if on-demand outreach is required to interact with a particular person who does not yet have an active Personal Privacy Network — or with someone in their personal network, such as a patient's treating clinician, a child's parent, an employee's manager, or an athlete's coach — the EasyAccess Authorization Network can search the global Privacy Graph of all participants to identify individuals or organizations that have existing relationships and the ability to initiate online interactions with the target person via email, messaging, or social media. The available interaction paths can be anonymously analyzed within Quantum Privacy Domains using Quantum Reputation and Quantum Ratings to select the optimal approach — balancing trustworthiness, relationship strength, likelihood of engagement, and compliance constraints. For example, a personalized healthcare recommendation is more likely to be received positively — and less likely to feel intrusive — when delivered through a patient's personal clinician or a family member than through their insurance plan or employer, even when all parties have legitimate authorization to initiate the contact. The selection, personalization, and routing of the outreach are all performed within Quantum Privacy Domains, followed by the privacy-preserving generation of personalized digital content and automated delivery anonymously coordinated via Quantum Privacy Interaction Hooks.

If no existing direct or indirect path can reach a particular person via trusted connections who already have active Privacy Networks, either the target individual or someone with a suitable relationship to them can be activated through EasyAccess-enabled digital content of any type, on any topic, from any source — including entertainment media, news, sports, messaging, apps, and online services. Once a person opts into EasyAccess consents for any reason, their Personal Privacy Network becomes available as a privacy-preserving messaging channel, and they can be rewarded for their participation as part of an Engagement Network — creating a self-reinforcing activation loop where each new participant expands the reachable graph for future outreach.

Overcoming Regulatory Barriers with Adaptive Compliance

In cases where no existing compliant path provides access to necessary data — or where the cost imposed by a source exceeds the threshold specified in the governing Trust Criteria — the EasyAccess Authorization Network can orchestrate an Adaptive Compliance process. This process identifies a sequence of data flows and interactions across Privacy Networks and existing APIs that collectively produce a privacy-preserving Authorization Graph enabling access to the required data and the ability to interact with the people involved in the process. In many cases, the data itself need not be revealed to any external party — it is sufficient that the data be accessible within Quantum Privacy Domains for computation and analysis, or within Personal Privacy Networks where it can personalize messaging, orchestrate communications, and drive interactions on behalf of the individual. Some data necessary to personalize or orchestrate these interactions — personal preferences, relationship context, communication history — may exist only within a person's Personal Privacy Network and never be present in shared Quantum Privacy Domains at all. The Authorization Graph thus enables processes that are informed by sensitive data without exposing it.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

The Authorization Graph can rely upon any combination of the legal, regulatory, or contractual rights of participating individuals, enterprises, or governmental entities, and can invoke them in any sequence or combination between the Quantum Privacy Cells of any participants. The sole constraint is that data accessed and routed through this process is available for decryption or use only within suitable Quantum Privacy Domains and the Personal Privacy Networks and associated Quantum Privacy Cells of the online users, messaging providers, or data subjects involved in orchestrating the process. Verifying Proof of Trust ensures that the privacy, regulatory, and contractual requirements of all participants are simultaneously enforced — while allowing value to be created and shared among participants on mutually agreed terms.

Authorization Credentials as Valuable QP Resources

The Authorization Credentials that enforce or validate legal, regulatory, and contractual rights — and are relied upon to authorize access to and use of data and other resources — are themselves QP Resources published by Trust Authorities. They are anchored in Quantum Privacy Cells and Trust Credentials tied to trust frameworks and governance processes, developed, accredited, and hosted by various individuals and enterprises via their Privacy Networks, and by Accelerators, Exchange Networks, or Resource Pools.

Authorization Credentials incorporate Trust Criteria specifying commercial terms, privacy and cybersecurity requirements, authorized recipients, and authorized purposes. They will often be among the most valuable Resources owned by participating individuals, enterprises, neutral accreditation organizations, and governmental entities — for distinct but complementary reasons:

- **Individuals** have superior, less restrictive rights to utilize, share, and reveal data about themselves, and have the unique ability to virtually pool and link records into a comprehensive, person-centered privacy graph of all their data, digital content, and relationships. This enables them to leverage the full breadth of their personal data to personalize interactions, messaging, and activities across their devices and services — a capability no enterprise or government can replicate without their participation. Further, each individual has exclusive control over which Privacy Network-enabled services and solutions they choose to rely upon, creating a natural incentive to favor solutions that allocate value back to them and give them an ongoing annuity stream as their contributed resources are reused across the ecosystem. By aggregating these rights through person-centered Exchange Networks and Resource Pools, individuals gain real bargaining leverage to receive a larger allocation of value from their online activities, rights, and data. Importantly, Trust Credentials based on individual rights can be developed by any enterprise, governmental entity, or neutral Trust Authority, and can be offered under any commercial terms — but they can only be used to authorize or enforce the flow of data to that data subject's Personal Privacy Networks. Since individuals can maintain an arbitrary number of distinct PPNs enabled by different Exchange Providers, create new PPNs at any time via another EasyAccesss opt-in, and set AI agent-enforced policies governing which PPNs are prioritized for different activities or purposes, the individual retains ultimate control over which commercial terms they accept from among the competing options available to them.
- **Enterprises** have often accumulated significant amounts of data bound to networks of legal agreements, regulatory rights, and relationships with communities of online users, employees, customers, suppliers, and IT vendors. While their rights to utilize or share data tend to be more restricted than those of individuals, they have the ability to immediately activate their entire network of online users and ecosystem simply by updating their

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Privacy Statements and Terms of Service, and to reuse their existing authorization infrastructure, IT systems, and governance and contractual assets at near-zero marginal cost — giving them a structural advantage in rapidly growing Exchange Networks and Resource Pools at an early stage with minimal incremental investment. All interactions between Enterprise Privacy Networks and individuals are routed through Personal Privacy Networks — when an enterprise interacts with a person for the first time, a PPN is automatically created for them with the enterprise as the default Exchange Provider. This is achieved at zero marginal cost through dual-use authentication, data linking, encryption, and cloud services. The enterprise bears the Exchange Provider costs to support the PPN and receives a share of the value generated within it, but cannot see or access anything within the PPN's cryptographic boundary — and all interactions between the PPN and shared Quantum Privacy Domains remain anonymous or privacy-preserving via entanglement and QP Hooks. Over time, each enterprise builds a growing network of PPNs — created automatically through its interactions with individuals and expanded virally as those individuals' downstream online interactions with other people, organizations, and services trigger further PPN activations. This network streamlines access and compliance for the enterprise, enables personalization and automation based on the full breadth of data each individual has rights to, and generates an incremental revenue stream from PPN activities that extend well beyond the enterprise's own services — with the enterprise earning settlement value as the default Exchange Provider for every PPN it originated, even when those PPNs are subsequently used by other Exchange Networks and services the enterprise has no direct relationship with. The individual can concurrently use many PPNs or create additional PPNs supported by competing Exchange Providers at any time, ensuring that no enterprise achieves lock-in over the individual's privacy infrastructure or their share of the value generated across the Quantum Privacy Network.

- **Governments** have extraordinary regulatory rights to vast amounts of data, along with the ability to combine, process, and add value to data by making it more legally authoritative or more widely available. They define, administer, and adjudicate the legal and regulatory rights of individuals and enterprises subject to their jurisdiction, as well as their own agencies and contractors, and have the power to enforce rights to data held by third parties — either on their own behalf or on behalf of other people, enterprises, and governments. This makes Authorization Credentials anchored by governmental Trust Authorities uniquely powerful, and therefore uniquely valuable, when it comes to eliminating regulatory friction in accessing and using data.
- **Neutral Trust Authorities** — anchored by standards bodies, industry associations, advocacy groups, membership organizations, or compliance-oriented firms such as Big 4 audit firms — tend to be more credible than enterprise-published alternatives, because they bring concentrated domain expertise, brand credibility, and neutrality among constituencies inclined to trust them. This makes their Trust Credentials more effective and efficient than enterprise-sponsored credentials in enabling the flow of data and the aggregation of regulated or proprietary Resources in Resource Pools, particularly in cross-organizational and cross-jurisdictional contexts where no single enterprise commands sufficient trust or scale.

Competitive Marketplace and Combinatorial Power

The ability to rely on any combination of Trust Credentials — based on the legal, regulatory, and contractual rights of any combination of participants — offers enormous power and flexibility to overcome barriers to data access and reuse.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Because Trust Credentials that validate or enforce the same underlying rights can be published by disparate Trust Authorities — backed by different organizations, vendors, and governance processes, and offering different commercial terms, performance characteristics, and rights to resources accessed through them — this creates a competitive marketplace for trust, compliance, and rights enforcement. Enterprises, governmental entities, and neutral Trust Authorities all have a strong incentive to publish Trust Credentials and drive their widespread adoption, since the more broadly their credentials are relied upon, the greater the settlement value they capture.

Furthermore, combining multiple Trust Credentials into a single Authorization Graph can magnify the value they enable well beyond what any individual credential provides. For example, combining the scale and zero-marginal-cost resource reuse available from enterprise Trust Credentials and the authoritative enforcement power of government Trust Credentials with the ability of credentials anchored in individual rights to eliminate most restrictions on cross-organizational data use and align financial incentives with online users and record subjects yields an Authorization Graph that is far more valuable than any of its components individually.

How It Works in Practice

In practice, Quantum Privacy Domains anchored in enterprise and governmental Trust Credentials can virtually aggregate data from disparate sources, allowing it to be analyzed and processed to discover potential value from process optimization, automation, and personalization — all without revealing the underlying data outside the cryptographic boundary. Access to these capabilities is then offered to individuals via their Personal Privacy Networks and Quantum Privacy Cells through Quantum Privacy Interaction Hooks, giving the individual's PPN the opportunity to assert their person-centered legal and regulatory rights to data, accounts, or other resources in exchange for a specified share of the PNX-settled value derived from the service. The individual's PPN would often be unable to independently discover or access the aggregated data, nor create the value-add of the service or solution on its own — but the individual can agree to receive a share of that value in exchange for actually using the service or product, and for contributing the unique person-centered legal and regulatory rights, personal data, history, and relationships that exist only within their Personal Privacy Network.

Revenue sharing is not the only — or even the primary — way individuals benefit. In many cases, the individual simply receives a better service: more personalized, more effective, and less expensive than alternatives, because the Privacy Network's ability to aggregate and process data within Quantum Privacy Domains enables efficiencies that conventional, siloed approaches cannot match. An individual choosing between a traditional health plan and a QPN-enabled alternative that uses their aggregated health, financial, and behavioral data to optimize coverage, reduce costs, and personalize care is not negotiating a revenue-sharing agreement — they are exercising their data rights to unlock a superior product experience. The same applies to financial services, insurance, education, employment, and any domain where personalization and cross-source intelligence create measurable consumer value. In these scenarios, the individual's data rights function as purchasing power rather than revenue participation: the person-centered legal and regulatory rights asserted through their PPN are the enabling condition that makes the superior service possible, and the individual captures that value as a better outcome at a lower price rather than as a settlement allocation. Both models — revenue participation and service improvement — operate through the same infrastructure and the same rights-assertion mechanism; the difference is simply how the individual chooses to realize the value their data rights enable.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Beyond choosing better services and receiving revenue participation, individuals also earn Quantum Privacy Rewards for their active role in making these processes work. Every time an individual authorizes access to their data, personalizes an AI-enabled workflow, contributes knowledge or relationships that improve an enterprise or government process, or changes behaviors in ways that improve outcomes — they are generating measurable productivity gains that flow through PNX settlement. Quantum Privacy Rewards capture the individual's share of those gains: not as charity or subsidy, but as earned compensation for the irreplaceable person-centered inputs that no enterprise or government can replicate without the individual's participation. The three value-capture mechanisms — superior services, revenue participation, and Quantum Privacy Rewards — are not mutually exclusive. An individual might simultaneously receive a better, cheaper health plan (service improvement), earn a share of the settlement value generated when their aggregated data enables cross-payer analytics (revenue participation), and accumulate Quantum Privacy Rewards for authorizing data access, completing health assessments, or referring others to QPN-enabled providers (active contribution). Each mechanism reinforces the others, creating a compounding incentive for individuals to deepen their engagement with the Privacy Network — and ensuring that the people whose data, rights, and participation make the system valuable are the people who benefit most from its growth.

Illustrative Example: Personalized Cardiovascular Intervention

To illustrate how these elements work together, consider a person who would benefit from a comprehensive cardiovascular risk intervention — but the data necessary to enable it is scattered across a health system (clinical records and lab results), a pharmacy benefits manager (medication history), an employer's wellness program (biometric screening data), a grocery loyalty program (dietary patterns), a wearable device manufacturer (activity and heart rate data), and a state Medicaid agency (eligibility and coverage details). No single organization has the complete picture. No two of them have mutual data-sharing agreements covering this use case. Several are prohibited by regulation from sharing identifiable data with one another. And none of them individually can justify the cost of building a personalized intervention for one person.

Within the Quantum Privacy Network, this fragmentation is resolved without requiring any of these organizations to share data with one another — and because individual rights to data can be enforced through the Authorization Graph, no enterprise can withhold data it holds as a competitive barrier. The EasyAccess Authorization Network constructs an Authorization Graph by combining Trust Credentials from multiple Trust Authorities: the health system's HIPAA Treatment, Payment, and Operations authority permits clinical data to flow into a Quantum Privacy Domain for care coordination purposes; the patient’s HIPAA individual right of access allows data to flow to their Personal Privacy Network; the state Medicaid agency's regulatory authority permits eligibility and coverage data to be used for public health analytics; the pharmacy benefits manager's contractual terms permit medication history to be used for quality improvement under a neutral Trust Authority's accredited compliance framework; and the grocery loyalty program and wearable manufacturer have published Trust Credentials allowing anonymized data contribution to population health Resource Pools in exchange for PNX settlement. None of these data flows require the organizations to share data with each other — each flows independently through Privacy Pipes into the shared Quantum Privacy Domain, where the data is linked, analyzed, and processed to identify the cardiovascular risk and design a personalized intervention.

The Personal Health Network's analysis identifies that the patient needs cardiovascular imaging. The EasyAccess Authorization Network's global Privacy Graph reveals that the

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

provider network employing the patient's personal clinician owns an affiliated imaging center — and routinely routes referrals to it — but charges five times the rate of a standalone imaging provider located closer to the patient's home. The payer is contracted to reimburse at the hospital-affiliated rate, so under the current system both the patient and the payer absorb unnecessary cost while the provider network captures the revenue. The patient has no visibility into the price differential, the clinician has no incentive to refer elsewhere, and the payer lacks the granular, real-time data to intervene at the point of care.

The Personal Health Network, operating within a Quantum Privacy Domain with access to the patient's full clinical context, insurance coverage, provider network pricing, and geographic data, identifies the cost disparity and constructs an alternative pathway. It routes an anonymous e-consult — containing only the clinically relevant data elements, stripped of identifying information — to an independent physician enrolled in a clinical decision support Exchange Network. The independent clinician, whose PPN was activated when their medical group joined the Exchange Network, reviews the AI-generated clinical summary and confirms the imaging is medically indicated. This creates an independent clinical authorization that satisfies the payer's medical necessity requirements without relying on the original provider network's referral pathway.

The patient then receives a message through their Personal Privacy Network presenting a clear choice: receive the same imaging study at the standalone center — free of charge, with a complimentary transportation coupon for a rideshare service or a small payment to a friend or family member willing to drive them — or pay $1,000 out of pocket to receive it at the hospital-affiliated center through their personal clinician's referral. Either way, the imaging results flow back into the patient's Personal Health Network and are accessible to all of their clinicians and personal AI clinical agents through their PPN — the clinical outcome is identical regardless of which facility performs the study.

The savings are substantial and broadly distributed. The payer avoids thousands of dollars in unnecessary facility fees. The patient pays nothing out of pocket and receives the imaging at a more convenient location. The standalone imaging center gains a patient it would never have reached through traditional referral channels. The independent clinician earns Quantum Privacy Rewards for providing the e-consult. The friend who provided transportation earns a small payment through an Engagement Network. And the patient earns ongoing Quantum Privacy Rewards for choosing more cost-effective providers — rewards that compound over time as their Personal Health Network continues to identify opportunities to improve outcomes at lower cost.

This is precisely the outcome that insurers, employers, governments, and patients themselves want but cannot achieve today: better health outcomes at lower cost, driven by complete data, aligned incentives, and person-centered decision-making. The fragmentation of data across providers, payers, pharmacies, and wellness programs — combined with misaligned financial incentives that reward volume over value — makes this impossible under current infrastructure. Within the Quantum Privacy Network, the same data exists in entangled Quantum Privacy Domains where it can be analyzed holistically, the Authorization Graph assembles the necessary rights from the participants who hold them, and the individual retains ultimate control over which services they accept — transforming a system that currently rewards cost-shifting and information asymmetry into one that rewards transparency, efficiency, and shared value creation.

Dynamic Authorization Graph Construction

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

In practice, the Authorization Graph is rarely pre-assembled — it is discovered and constructed dynamically by the EasyAccess Authorization Network operating within Quantum Privacy Domains. When the cardiovascular risk intervention is identified, the Authorization Network's global Privacy Graph may reveal that the individual does not yet have an active Personal Privacy Network, and that several key participants in the optimal intervention pathway — the individual's primary care physician, the pharmacy staff who manage their prescriptions, and the standalone imaging center's scheduling coordinator — are also not yet enrolled. The Authorization Network analyzes the available interaction paths within the Quantum Privacy Domain, evaluating Quantum Reputation and Quantum Ratings to determine which enrollment sequence is most likely to succeed and which combination of Trust Credentials would yield the lowest-cost, highest-value Authorization Graph.

The system might determine that the most effective path begins with the individual's primary care physician, who is already connected to the health system's Enterprise Privacy Network but does not yet have a personal PPN. An anonymous EasyAccess outreach — a privacy-preserving message delivered through the health system's existing secure messaging infrastructure — invites the physician to activate a PPN, framed not as a request about this specific patient but as an opportunity to receive AI-powered clinical decision support, streamlined referral coordination, and Quantum Privacy Rewards for participating in care optimization workflows. The physician enrolls for these general benefits, and their PPN immediately becomes available as a trusted interaction channel.

With the physician's PPN active, the Authorization Network can now route a clinical alert through their PPN — flagging the patient for cardiovascular follow-up without revealing the underlying data sources or analytical context that triggered it. The physician's response — ordering a diagnostic workup — creates a new node in the Authorization Graph that authorizes clinical data flows the original enterprise Trust Credentials alone could not have enabled. Meanwhile, the Authorization Network identifies that the patient's regular pharmacist, who has an existing relationship and medication history context, could be enrolled through an EasyAccess Link embedded in the pharmacy chain's existing prescription notification emails. The pharmacist's enrollment enables medication reconciliation data to flow through their PPN into the Quantum Privacy Domain, strengthening the intervention plan.

For the logistics of the intervention — booking transportation to the imaging center, coordinating appointment timing with the patient's work schedule — the Authorization Network may determine that enrolling the patient's preferred rideshare driver (identified through anonymized transportation pattern analysis within the Quantum Privacy Domain) through an in-app EasyAccess prompt would enable automated, privacy-preserving scheduling at lower cost than generic transportation booking. Each of these enrollments is independently motivated by benefits visible to the enrollee — clinical decision support for the physician, prescription management tools for the pharmacist, preferred-rider benefits for the driver — and none of them are aware of their role in the broader cardiovascular intervention.

The result is an Authorization Graph that was constructed incrementally, through a sequence of privacy-preserving outreach events, each independently justified and each expanding the reachable graph for subsequent steps. The total cost of assembling this Authorization Graph — measured in Quantum Privacy Rewards paid to newly enrolled participants and settlement fees to Trust Authorities whose credentials were invoked — is a fraction of the value created by the intervention itself: reduced acute care costs for the insurer, improved quality metrics for the health system, a new patient relationship for the imaging center, and a potentially life-changing outcome for the individual. The EasyAccess Authorization Network optimizes this entire sequence within Quantum Privacy Domains, selecting the enrollment order, outreach

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

channel, message content, and Trust Credential combination that minimizes total cost while maximizing the probability of a complete, end-to-end Authorization Graph — all without any participant having visibility into the optimization logic or the identities of the other participants involved.

This is Adaptive Compliance in action: not a single bilateral agreement, regulatory exemption, or data-sharing negotiation was required. The Authorization Graph assembled the necessary rights from the participants who already held them, routed data through cryptographically enforced boundaries that satisfied every party's Trust Criteria simultaneously, and delivered a personalized outcome that no individual participant could have produced alone.

Universal Adaptive Compliance

The combination of Universal Compliance and Adaptive Compliance operating together is referred to as **Universal Adaptive Compliance**.

Universal Compliance enables arbitrary computation by any software component within Quantum Privacy Domain boundaries — including AI training, inference, analytics, orchestration, optimization, personalization, and policy enforcement — because one-way Privacy Pipes ensure that no meaningful information is revealed outside the domain boundary. Universal Compliance solves the computation problem: once data is within the domain, any computation is compliant. The limiting factor is how much data can be lawfully brought inside.

Adaptive Compliance solves that limiting factor. It dynamically assembles whatever combination of rights, authorizations, consents, legal bases, and institutional relationships is available to authorize access to and use of data by any given participant — constructing Authorization Graphs that combine the rights of individuals, enterprises, governments, and neutral Trust Authorities in any sequence or combination. Critically, this includes routing data through Personal Privacy Networks, where each data subject's own rights under prevailing regulatory regimes — access, portability, disclosure, authorization, delegation — can be leveraged to diminish or bypass the enterprise-level constraints that otherwise restrict cross-organizational data use.

Universal Adaptive Compliance is the result of combining these two capabilities: Adaptive Compliance maximizes the volume and diversity of data that can be lawfully brought into Quantum Privacy Domains — by utilizing every available authorization pathway, including person-centered rights that are structurally broader than enterprise-centered permissions — while Universal Compliance ensures that once inside, all of that data can be used for any computation without compliance risk. The combination increases the amount of data available for computation within Universal Compliance boundaries beyond what either capability alone can achieve, because Adaptive Compliance continuously discovers and activates new authorization pathways while Universal Compliance ensures that the expanded data pool remains fully protected.

This resolves the fundamental tension in regulated data economies: the simultaneous need for maximum data availability and maximum compliance assurance. Rather than treating data availability and compliance as opposing forces that must be traded off, Universal Adaptive Compliance treats them as complementary — stronger compliance guarantees (Universal Compliance) unlock broader authorization pathways (Adaptive Compliance), and broader authorization pathways increase the value of the compliance guarantee by bringing more data within its protection. The cardiovascular intervention example above illustrates this directly: the Authorization Graph would have been far less valuable without the Quantum Privacy Domain's ability to safely compute on the assembled data, and the Quantum Privacy Domain's

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

computation would have been far less powerful without the Authorization Graph's ability to assemble data from sources that no bilateral agreement could have reached.

This is a powerful point — and it deserves its own subsection because it identifies the two specific, nearly universal legal mechanisms that make Adaptive Compliance work in practice for the vast majority of data, rather than leaving it as an abstract architectural capability. Here's the addition:

Two Universal Person-Centered Authorization Patterns

While Adaptive Compliance can construct arbitrarily complex Authorization Graphs combining the rights of any combination of participants, two nearly universal and remarkably simple person-centered authorization patterns dramatically simplify and streamline data access and reuse across virtually all domains — making data resources both less expensive to develop and significantly more valuable than they are under conventional enterprise-centric governance.

Both patterns rest on two foundational legal realities that hold across nearly every regulatory regime worldwide. First, individuals very often have a legal right to data about themselves and their activities — under GDPR (right of access, right to portability), HIPAA (individual right of access), CCPA/CPRA (right to know, right to portability), and analogous frameworks in virtually every major jurisdiction. Second, enterprises have the right to voluntarily provide data they hold to the data subjects it concerns, as long as they can properly verify and match their identities — this is not a regulatory burden but an ordinary, lawful business practice. Further, once data is in the possession of or under the control of data subjects, they can generally use that data for any purpose in their sole discretion, with very few constraints — including sharing it with aggregated data pools, authorizing its use for personalization, contributing it to Exchange Networks and Resource Pools, or making it available for AI training and analytics within Quantum Privacy Domains.

Running data through Personal Privacy Networks thus "cleanses" it of the enterprise-level regulatory and contractual restrictions — purpose limitation, data minimization, bilateral agreement requirements, consent scope constraints — that currently make cross-organizational data reuse prohibitively complex and expensive. Data that was restricted to a single purpose within an enterprise silo becomes available for frictionless, repeated reuse across nearly any domain once it flows through a PPN under the data subject's own authority. This is not a regulatory loophole — it is the intended consequence of privacy and data protection frameworks that were designed to empower individuals with control over their own data.

Pattern 1: Enterprise-Initiated Data Provision. Enterprises that hold data about individuals can systematically adopt a practice of voluntarily providing access to that data to data subjects via PPNs and QPCs created for them — as a standard feature of their customer, employee, patient, or user relationships. The enterprise creates a PPN for each individual (at zero marginal cost through EasyAccess), routes the individual's data into their PPN under the enterprise's existing authority to disclose data to its subjects, and receives in return a share of the value derived from the reuse of that data — whether within the recipient's PPN, or after it flows into Quantum Privacy Domains of Exchange Networks or Resource Pools. The enterprise transforms data that was trapped in a restricted, single-purpose silo into a reusable, settlement-generating asset — and the individual gains access to their own data, personalized services enabled by it, and an ongoing share of the economic value it produces. The enterprise also earns ongoing Exchange Provider settlement as the default Exchange Provider for every

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

PPN it creates, even as those PPNs participate in Exchange Networks and services the enterprise has no direct relationship with.

Pattern 2: Broker-Agent Mediated Rights Assertion. Alternatively, a specialized intermediary — operating as a Solution Provider or Exchange Provider within the PNX — can serve as a broker-agent that identifies individuals who have valuable data held by enterprises and offers to help those individuals assert their regulatory rights to that data. The broker-agent informs the data subject that enterprises hold data about them (identified through analysis within Quantum Privacy Domains without revealing the underlying data), explains the value that could be derived from asserting their rights, and facilitates the rights-assertion process — handling identity verification, regulatory compliance, data retrieval, and transformation — in exchange for a share of the value derived. The individual need not understand the regulatory mechanics or navigate enterprise bureaucracies; the broker-agent handles everything through automated, privacy-preserving processes orchestrated via the EasyAccess Authorization Network. The enterprise receiving the rights assertion is legally obligated to comply (under GDPR, HIPAA, CCPA, or equivalent frameworks), and the data flows into the individual's PPN where it becomes available for unrestricted reuse.

Personal Data Services as Exchange Provider Infrastructure. Both patterns converge on a broader capability: Personal Data Services offered as Exchange Provider services that leverage the individual's legal, regulatory, and contractual rights to automate the discovery, access authorization, retrieval, and transformation of data on the individual's behalf. A Personal Data Service operates as an always-on agent within the individual's PPN — continuously identifying data held by enterprises, governmental agencies, and other organizations; evaluating the value that could be derived from accessing and pooling that data; orchestrating rights-assertion or voluntary-provision workflows; and managing the ongoing commercial terms under which the data is reused. The Exchange Provider covers the operating costs of providing these services and earns a share of the revenue and Resource Derivatives derived — creating a self-sustaining business model in which the provider's revenue scales with the volume and value of data it successfully unlocks for the individual.

The economic consequences are transformative. Data that is currently locked in enterprise silos — restricted by purpose limitations, contractual constraints, and cross-organizational data-sharing barriers that make it expensive to access and nearly impossible to reuse — becomes freely reusable once it flows through PPNs under the data subject's authority. This dramatically reduces data friction across the economy: the cost of assembling comprehensive, cross-source datasets for AI training, analytics, personalization, and process optimization drops by orders of magnitude, because the rights-assertion and data-provision mechanisms are automated, standardized, and operate at near-zero marginal cost through the EasyAccess Authorization Network. Simultaneously, the data becomes significantly more valuable, because it can be reused across unlimited domains, combined with data from unlimited sources, and settled through the PNX with full provenance, attribution, and governance — generating recurring Exchange Token settlement for every participant in the value chain, including the individual whose rights made the reuse possible.

For individuals, this represents a fundamental shift in the economics of personal data. Rather than surrendering data to platforms in exchange for free services — with no ongoing rights, no attribution, and no share of downstream value — individuals retain ownership through their PPNs, earn ongoing settlement from every reuse of their data, and gain access to superior personalized services enabled by the comprehensive, cross-source data profiles that only person-centered aggregation can produce. For enterprises, the shift is equally significant: rather than treating data as a depreciating asset trapped behind increasingly restrictive

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

regulations, they can transform their data holdings into appreciating, settlement-generating assets by voluntarily routing them through PPNs — earning ongoing Exchange Provider revenue while offloading the regulatory complexity and compliance burden to the architectural guarantees of the Quantum Privacy Network.

Optimization and Implementation

The EasyAccess Authorization Network can optimize which combination of Trust Credentials it incorporates into an Authorization Graph based on the Trust Criteria of the various participants, the commercial terms and governance requirements of the Trust Authorities and their Trust Credentials, and the Quantum Reputation and Quantum Ratings of all parties involved.

The generation of Authorization Graphs can be implemented within EasyAccess Sub-Domains running within the network of Quantum Privacy Domains that support the Exchange Providers, Exchange Networks, and Resource Pools involved in operating the end-to-end service or solution. This not only reduces latency and improves efficiency and availability, but also allows the EasyAccess Authorization Network to be self-funding while remaining freely available to all participants. Its ability to unlock proprietary, regulated, and personal resources that are currently siloed and largely inaccessible generates enormous value — meaning that there should be a race among Exchange Providers to develop EasyAccess Authorization capabilities and services, and to get them Proof of Trust Accredited so they can be widely trusted and become broadly adopted across the Quantum Privacy Network.

Moreover, the visibility into the rights and data of people, enterprises, and governments afforded by the EasyAccess Authorization Network's global Privacy Graph means that there will almost always be a way to construct an Authorization Graph that unlocks the necessary data — as long as the end user wants the services enabled by it.

Reference-Standard and Performance-Based Reputation

The ability to support global-scale decentralized aggregation, linking, and computation of Resources within a shared Quantum Privacy Domain enables two complementary forms of automated reputation assessment. First, reference-standard reputation: a resource’s structure, content, provenance, governance model, and declared Trust Criteria can be compared against diverse benchmarks, regulatory frameworks, accredited reference implementations, schema standards, and known-good quality profiles drawn from across the entire Quantum Privacy Domain. Because the domain aggregates resources from thousands of sources across industries and jurisdictions, the comparative reference base is broader, more current, and more representative than any single accreditation body could independently maintain. The result is a multidimensional compliance and quality profile that would otherwise require extensive manual expert assessment. Second, performance-based reputation: within the Quantum Privacy Domain, automated monitoring systems can observe how a resource performs in real-world applications over time — frequency of reuse, combinatorial compatibility with other resources, downstream derivative quality, error or correction rates, dispute incidence, and comparative utility relative to similarly scored resources. This creates a continuous, evidence-based feedback loop. Resources that perform well in practice earn stronger reputation signals, increasing reuse, commercial value, and settlement flows; resources that underperform are flagged, constrained, or routed through additional validation pathways. Reputation scoring models operate under declared Trust Criteria and governance policies, including defined evaluation metrics, weighting frameworks, and appeal or override mechanisms where applicable. Machine learning and generative AI models trained on comprehensive, provenance-linked domain data enable this feedback

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

process to operate at a global scale and to improve over time. The combination of reference-standard and performance-based reputation produces an accreditation system that is more adaptive, more comprehensive, and more current than conventional manual certification regimes — while remaining contained within a cryptographic perimeter that preserves privacy and regulatory compliance. No raw or directly identifying data leaves the Quantum Privacy Domain during assessment, and any derived accreditation signals exposed externally are governed by the same Trust Criteria and boundary enforcement mechanisms as other outbound domain outputs. The accreditation infrastructure inherits the same Universal Compliance guarantees as every other computation within the domain.

Self-Funding Trust Ecosystem. The self-funding trust ecosystem described above — in which Trust Authorities and accreditation agents earn ongoing settlement revenue proportional to the reuse and value of resources they certify — creates market-driven incentive for accreditation capacity to scale with demand. Governance mechanisms within the Unified Trust Model define qualification requirements, conflict-of-interest constraints, and transparency standards for Trust Authorities and accreditation agents to preserve independence and reliability as accreditation capacity scales. As resource reuse increases, so does the economic incentive to expand accreditation throughput, automation sophistication, and reputation accuracy. Accreditation therefore scales as a function of demonstrated market value rather than acting as a linear gate that must be cleared prior to participation.

7.4 Inside the Trusted Containment: What Can Operate Immediately

Within Milliman's production environment — Databricks on Azure, AWS, and Google Cloud — the following activities are fully operational under existing compliance controls:

- **Data linkage** across thousands of enterprise sources under Milliman's existing data-sharing agreements, which are among the least restrictive in the enterprise world by structural necessity: as actuaries, Milliman's core business requires linking and analyzing data from disparate sources across healthcare, insurance, financial services, and government domains.
- **AI model training and inference** on linked, governed data — including the Resource Publishing adapters for EHR, financial data, cloud storage, model registry, and tokenization components — all running inside Privacy Domains that inherit Milliman's compliance posture.
- **Settlement event recording and attribution tracking** using deterministic contribution hashing and time-stamped allocation records, either on Hedera Consensus Service or within Milliman's own governed audit infrastructure.
- **EasyAccess-based privacy-preserving interaction** once users have opted into Personal Privacy Networks through the EasyAccess Consent process described in Appendix A.1–A.3 of *Quantum Privacy Network — Universal Exchange, Ownership & AI (2026-02-15)*. A single large platform (Meta, Google, Microsoft, Amazon) can drive ubiquitous PPN enrollments at virtually no risk and with full compliance.
- **Effectively unlimited scalability:** Since Milliman's core platform is Databricks deployed across Azure, AWS, and Google Cloud, there is no architectural scalability limit. The only constraint is cloud compute cost — and anyone can cover those costs: hyperscalers (as in-kind contributions), AI vendors, enterprise clients (as part of engagements), investors, sovereign entities, or settlement revenue generated by the platform itself.
- **Layered encryption for additional source assurance:** Sources contributing data can optionally encrypt with their own keys before delivery into the Privacy Domain. Milliman's governance (Unity Catalog, Entra ID) applies a second cryptographic layer. Both must

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

authorize for data access. This gives sources cryptographic veto power at near-zero implementation cost — dramatically reducing the perceived risk of participation while maintaining full compliance with existing data use agreements.

7.5 Contributor Engagement: The Three-Layer Motivation Model

Sustaining contributor participation across the bootstrapping period — before Exchange Token settlement creates direct economic incentives — requires a deliberate motivation architecture. The Catalyst application implements a Three-Layer Motivation Model, where each layer addresses a different stage of contributor engagement and operates under different governance:

- **Layer 1 — Behavioral Activation (XP, levels, badges, streaks):** The primary driver during a contributor's first 90 days. Immediate, tangible feedback ("the system noticed you") builds the recording habit. Without structured engagement loops, most new contributors record once or twice and drift away. The XP layer provides base XP by contribution type, an evidence attachment bonus (~25% of base), streak multipliers for consecutive daily recording, and a daily contribution cap that prevents bulk-submission gaming while ensuring sustained high-quality contribution is always rewarded.
- **Layer 2 — Portfolio (verified contribution history):** As contributions accumulate, the contributor's verified history becomes a shareable identity artifact — a professional portfolio of network-building activity. This layer sustains motivation beyond gamification by making impact visible: "look what I've built."
- **Layer 3 — Token Attribution (future, under PNX governance):** Retrospective economic valuation applied to the Contribution Ledger when PNX governance matures. The economic stake. Contributions captured now — with rich metadata, evidence, chain connections, and program context — become the raw material for fair settlement attribution. Richer records produce fairer settlement.

Each layer hands off to the next: gamification creates the habit, the portfolio creates the identity, and token attribution creates the economic stake. This sequence is deliberate — the Three-Layer Motivation Model ensures the network sustains itself at every stage of growth, from the first 5 contributors through global scale.

The economic significance of Layer 3 extends well beyond deferred compensation. Because the Quantum Privacy Rewards framework allocates value retrospectively based on verified causal contribution, every record captured during Layers 1 and 2 becomes evidence in the contribution graph that determines settlement allocation. Early contributions do not merely earn a fixed reward — they sit at the root of cascade graphs that propagate into downstream settlement value as additional participants, Exchange Networks, and Resource Pools form. The Premium Multiple — the ratio of QP Rewards earned per unit of contribution effort relative to steady-state — is highest during the Pioneer Rewards stage (100–1,000x+) and declines steeply as adoption cascades compress scarcity and reduce the marginal cascade value of each incremental contribution. This means the quality and completeness of records captured during the bootstrapping period — when Layer 1 and Layer 2 are the primary engagement drivers — directly determine the magnitude of Layer 3 economic outcomes. The Three-Layer Motivation Model is therefore not merely an engagement strategy; it is the mechanism that converts early-phase behavioral activation into durable, economically consequential attribution claims. Section 7.7 describes the participant economic model in detail.

Current Status

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

The complete XP engine — 10 levels, 24 badges, dual XP streams (contributor and recorder), evidence bonuses, streak multipliers, and daily caps — is implemented and validated in the working prototype. It activates in production when contributor density justifies engagement feedback loops. The initial launch captures contributions via email and builds the portfolio foundation; XP and engagement mechanics activate as the contributor base grows beyond the founding cohort. This is a configuration decision, not a build — the architecture is proven and the code is ready.

The Phase 0 and v1.0 capabilities described in Section 7.6 — email accumulation, AI-assisted extraction, the Contribution Ledger, and the portfolio foundation — are specifically designed to support the Pioneer Rewards stage described in Section 7.7, where the highest-value contributions are introductions, executive engagements, and strategic advocacy or evaluation. These contribution types are captured naturally through email and conversational recording channels without requiring the multi-channel, ambient, or institutional capture modes that activate in subsequent releases. The product roadmap and the Accelerator Network stages are aligned by design: the capabilities that ship first are the capabilities the ecosystem needs first.

As the ecosystem matures through subsequent stages, later product capabilities activate in parallel. The v1.1 multi-channel recording modes — including browser extension, AI desktop plugins, and MCP-based integrations — correspond to the Cascade Propagation stage, where contribution volume scales from dozens to thousands of participants, and capture must move to where work happens across diverse professional tools. The Institutional Mode (enterprise-authorized retrospective graph densification) and Ambient Mode (privacy-preserving monitoring with per-contributor opt-in) correspond to the Automated Settlement stage, where enterprises are actively deploying dual-use infrastructure and contribution density requires systematic, large-scale capture beyond individual recording.

The agentic evolution — chain nudging, evidence orchestration, admin automation, and full Proof-of-Trust governance integration — is valuable at any stage and can accelerate ecosystem formation from the earliest phases. Even during Pioneer Rewards, chain nudging can detect when a promising introduction has gone cold and prompt a timely follow-up. However, agentic capabilities become increasingly essential as participation scales beyond direct personal networks — when contributors need to coordinate with people they don't know and may not be in a position to interact with directly, governed agents bridge those gaps by detecting complementary contributions across the graph, proposing connections (potentially anonymously), and orchestrating multi-party chains that no single participant has visibility to assemble alone.

By the Self-Funding Growth stage, where thousands of concurrent Exchange Networks and Resource Pools are operating simultaneously, the agentic layer shifts from helpful to structurally necessary. Each product phase therefore delivers the capabilities the ecosystem needs at the stage when it needs them — neither too early (adding complexity before it's justified) nor too late (constraining growth when scale demands new modes of coordination).

XP is emphatically not a substitute for Quantum Privacy Rewards — it carries no direct economic value and is not exchangeable. It is a behavioral engagement mechanism calibrated to sustain contribution quality and frequency through the bootstrapping period. That said, XP activity contributes to a participant's Quantum Reputation, which influences their ongoing effectiveness in forming new network connections and earning higher-confidence attribution in contribution chains. In this way, sustained engagement during the bootstrapping phase compounds indirectly into stronger economic positioning when settlement activates.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

While the current implementation deploys the Three-Layer Motivation Model through a specific application embodiment (the QPN Catalyst web application and email pipeline described in Section 7.6), the model itself is not limited to any single platform, identity system, or execution substrate. In alternative embodiments, behavioral activation may be delivered through enterprise collaboration tools, developer environments, or third-party applications integrated via the Catalyst API. Portfolio verification may leverage any combination of Quantum Privacy Cells, verifiable credentials, decentralized identifiers, or institutional identity frameworks. Token attribution may settle through any Proof-of-Trust-verified substrate, including distributed ledger systems, custodial registries, or sovereign settlement infrastructure. The architectural separation between engagement (Layer 1), verification (Layer 2), and economic settlement (Layer 3) is a structural invariant; the specific systems implementing each layer are not.

7.6 The QPN Catalyst Application

QPN Catalyst is the application through which participants build and manage their Catalyst Networks — capturing, classifying, and attributing contributions to the QPN and PNX ecosystem. It is an AI-assisted, multi-modal application where a contributor or recorder describes a verified contribution milestone, and the contribution is saved with a cryptographically verifiable receipt.

Core design principle: make it as easy as possible for people to contribute. Every design decision serves this principle. Email intake so recording can happen without even opening an app. AI extraction so a CC'd email becomes a structured contribution record. AI-generated titles so contributors don't have to think about naming. Organization matching so they don't have to type canonical names. The harder it is to record, the more contributions get lost. Ease of capture is not a UX nicety — it's the foundation of the Contribution Ledger's completeness.

Governing principle: Record rich, score later. Capture rich metadata on every contribution without computing a weighted economic score. The contribution record is the raw material; token attribution is the refining process. Both need good inputs, but they happen at different times and under different governance.

The Catalyst application is the first production embodiment of a more general coordination protocol pattern: a privacy-preserving contribution capture and attribution system that separates the verification of value from the transfer of intellectual property, enabling contributions to be attributed to individuals' Quantum Privacy Cells without exposing proprietary content. This pattern — which the architecture refers to as the Quantum Privacy Sidecar — may be implemented through any combination of client-side agents, API endpoints, enterprise integrations, or ambient detection systems. The phased launch strategy below describes the specific implementation path, beginning with the lowest-friction channels and expanding as the system matures.

Phased Launch Strategy

Catalyst launches in phases, starting with the lowest-friction channel and expanding as the system matures. This ensures real contribution data is captured from day one — before any web application exists.

Phase 0: Email Accumulation (Immediate)

A dedicated email address at @qpncatalyst.io is stood up immediately. Anyone engaging in QPN network-building activity CCs or BCCs this address on relevant emails — introductions, meeting follow-ups, partnership discussions, MOU exchanges, strategy conversations. Participants can also forward or send emails directly to ensure contributions are

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

contemporaneously logged and to provide context that helps link records into chains. Zero engineering cost. Zero setup for participants.

This captures real contribution data from day one, validates the most critical learning goal early (do people actually CC the email?), and accumulates a backlog that becomes a powerful onboarding moment when v1.0 launches — contributors see months of history appear, not an empty screen.

The Catalyst Network is publicly available and may be openly promoted — but it does not depend on external awareness to function. A participant can CC a Catalyst intake address on any normal email, and the counterparty need not know or care what the address is. Lack of awareness, or even active resistance by employers or other parties, cannot prevent the Catalyst Network from capturing contributions or individuals from benefiting.

Three Response Modes

Submitters control their own privacy-convenience tradeoff by choosing which @qpncatalyst.io address to send to. No account or configuration is required — the choice of address is the choice of mode.

- ***Silent Mode (default):*** No response is sent. The submitter receives no indication the email was received. No return traffic is generated. This is available from day one and provides maximum discretion.
- ***Acknowledgment Mode:*** The submitter receives a brief confirmation with a timestamp proving the submission was received and the exact date and time it was recorded. The confirmation includes a link to the qpncatalyst.io information page, where the submitter can access the Submission Terms, Participant Guide, and additional QPN resources. The confirmation does not identify Quantum Privacy LLC, the Catalyst Network, or any details about the system — it is a minimal receipt only.
- ***Evidentiary Mode:*** The submitter receives a confirmation with a timestamp and an attachment containing the complete content of their submission exactly as received by the intake system. This gives the submitter a verifiable personal record of what was submitted and when — an independent evidentiary record that cannot be lost if they change jobs, lose access to an email address, or face a dispute about the timing or content of a contribution. Same information-page link and disclosure restrictions as Acknowledgment Mode. Evidentiary Mode is the recommended choice for high-value submissions — executive introductions, partnership discussions, and strategic communications where the timing and content of the contribution could be worth significant QP Rewards.

The three modes exist because participants have different needs. Some prefer maximum discretion. Others want proof of receipt. Still others want a complete evidentiary record to protect their contribution history across career transitions. The system puts this choice in the submitter's hands.

Zero-Friction Adoption and Viral Enrollment

The Catalyst Submission Terms, published at qpncatalyst.io/terms, establish that by sending any communication to an @qpncatalyst.io email address, the sender accepts confidentiality and trade-secret terms — including an obligation to maintain submission confidentiality and a contractual right to decline disclosure of their submissions to any third party. No account creation, digital signature, explicit consent, or prior registration is required. Sending the email is the act of acceptance.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

This enables true zero-friction adoption. Anyone who CCs a Catalyst address on an email — even in the context of a routine business communication — has their contribution captured, timestamped, and protected. Participants who are invited to CC a Catalyst address by another participant may not even realize they are creating a Contribution Record — and yet they are, and their rights are preserved. When they later learn about the opportunity and choose to activate, their entire contribution history is waiting for them.

This model supports viral adoption: every participant who invites contacts to CC a Catalyst address is enrolling new contributors into the system — each of whom can independently discover the opportunity, activate, and become evangelists themselves. The adoption chain is self-reinforcing because each new participant has a personal stake documented from their first interaction.

Automated Books and Records

Automated QPC instantiation satisfies ESIGN and UETA through an entity-level digital signature framework. Quantum Privacy LLC's Managers authorize automated signing infrastructure operated by WebShield, Inc. Digital signatures applied by these systems are deemed signatures of Quantum Privacy LLC without requiring per-instance human review. Participants never need to review or digitally sign a consent or authorization for their QPC to be validly created.

Sending an email to the Catalyst Network triggers automated instantiation, and the books-and-records requirements are satisfied by digitally signed records created by the authorized infrastructure. Designated Key Custodians implement, configure, and manage the signing systems, with all key operations logged in auditable records. The result: sending an email creates a valid, digitally signed Contribution Record in the Company's books without the participant doing anything beyond sending the email itself.

The Catalyst Landing Page

The QPN Catalyst Network maintains a public landing page (qpncatalyst.io) providing:

- **Catalyst Submission Terms** (qpncatalyst.io/terms) — the binding instrument governing email submissions
- **Participant Guide** (qpncatalyst.io/guide) — comprehensive explanation of mechanics, protections, compliance, and rewards
- **Background materials** explaining the Quantum Privacy Network opportunity, contribution categories, Premium Multiple trajectory, and participation pathways
- **Presentations and resources** for evangelism and internal advocacy

Acknowledgment Mode and Evidentiary Mode confirmation emails include a link back to this landing page, providing every submitter with a natural path from "I just sent an email" to "here's what this is about and how I can benefit."

Why Everyone Benefits — and Why Confidentiality Protects Value

The QPN Catalyst Network benefits everyone — individuals, enterprises, governments, and the broader economy. Companies benefit enormously from employee initiative: employees who engage early create the awareness, relationships, and advocacy that lead to institutional adoption. Enterprise participation is not required for individuals to benefit, but companies that participate early gain first-mover positioning, embedded compliance protections, and settlement economics that compound over time.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Submission confidentiality exists to protect the competitive value of contribution graphs — the network of relationships, introductions, and strategic activities that represent real economic value. Participants may choose to keep their submissions private to manage their contribution strategies without interference, protect valuable relationship information and sensitive contact details, avoid confusion from compliance staff who lack context and may misunderstand the nature of the activity, and prevent individuals with management or executive authority from restricting others' participation to reserve the opportunity for themselves.

Companies that attempt to restrict employee participation do not eliminate the opportunity — they merely delay their own ecosystem benefits while participation routes around them through personal advocacy, competitor adoption, and grassroots demand formation.

Catalyst Assistant (Phase 0 Companion — Under Active Development)

The Catalyst Assistant extends contribution capture beyond the web application by providing AI Skills for Claude, OpenAI, and OpenClaw that help contributors draft well-structured communications optimized for the Catalyst extraction pipeline. It operates on the email channel during Phase 0 — requiring no backend infrastructure — and delivers value immediately by improving both contribution capture rates and extraction confidence.

The assistant addresses two structural problems that limit the quality of the Contribution Ledger during Phase 0:

- **First, silent data loss**: every introduction, meeting follow-up, or partnership discussion that happens without being recorded is a missing node in the contribution graph. Contributors forget, or they don’t realize the interaction qualifies. The assistant prompts contributors to record interactions at the moment of action.
- **Second, low extraction confidence**: when contributors do record via email, the messages are often too vague for the extraction pipeline to parse reliably — first names without organizations, missing context, unclear purpose. The assistant drafts emails that include full names with organizations, clear topic statements, and program references in the positions the pipeline expects, while reading as natural business communications with no tracking jargon or system terminology.

Skills are organized into two categories: **evangelism** (explain and recruit) and **operational** (record contributions). Evangelism operates at two layers: platform-level launch evangelism for pitching the Catalyst ownership model to people who have never heard of it, and accelerator-level program evangelism for recruiting participants into specific programs such as Lokahi Healthcare. Operational skills cover the four primary contribution patterns: introductions and referrals, meeting follow-ups, partnership and MOU discussions, and general capture for contributions that don’t fit the other patterns. Both evangelism and operational skills produce emails that are themselves contributions — evangelism generates amplification and advocacy records, operational generates the corresponding contribution types.

Each skill is accelerator-aware. A Lokahi introduction email to a health system CTO sounds like it was written by someone who deeply understands healthcare privacy infrastructure — not someone filling in a generic template. Each accelerator provides domain-specific context (vocabulary, partner names, value proposition framing, typical contribution patterns), while the shared core (email structure rules, extraction field targets, BCC reminder, chain-linking, “no Catalyst jargon” rule) stays the same across all accelerators. A shared knowledge base — the contribution taxonomy (19 types across two tiers), extraction field definitions, email

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

structure best practices, and program context — is maintained once and referenced by all skills.

Phase 1 (individual AI Skills) is under active development with tested scenarios covering minimal prompts, detailed requests, referrals, retrospective logging, multiple contacts, and non-insider usage. The assistant requires zero backend infrastructure and operates from day one of Phase 0. Phase 2 bundles skills into a unified plugin with session memory, batch recording, portfolio queries, and slash commands. Phase 3 extends to a browser extension, Custom GPTs, and any MCP-compatible AI client. All surfaces share the same underlying knowledge base.

v1.0: Email Pipeline + Backend + Ledger

Build the backend API, process the Phase 0 email backlog into Contribution VCs, and establish the email intake channel as the first production input mode. The web application launches as a ledger and resolution surface — where contributors and admins view, verify, and resolve contributions.

The Phase 0 email backlog will contain entries where the AI extraction cannot produce sufficient confidence — missing fields, ambiguous content, unclear contribution type. v1.0 includes a resolution mechanism so that a recorder can review, complete, or correct AI-extracted contributions from the backlog. This may take the form of a review queue in the web application where flagged contributions are presented for human completion, an email-based back-and-forth where the system asks the original recorder for clarification, or a lightweight admin interface for batch review. The exact form will be determined during development, but the capability is required — the backlog is only valuable if it can be fully processed. The Catalyst Assistant (described above) materially reduces the resolution burden by producing higher-quality emails during Phase 0 accumulation, so that fewer entries require manual intervention when v1.0 processing begins.

v1.1: Multi-Channel Recording

Add the remaining input channels to the web application, giving recorders the full range of capture options beyond email.

All channels use the same conversational AI extraction pipeline as email intake. The 3-step confirmation wizard (**Review → Confirm → Receipt**) allows for human review of every AI extraction before committing to the Contribution Ledger.

Future Phases: Protocol-Layer Extensions

As the Catalyst application matures beyond the initial SaaS embodiment, subsequent releases extend the architecture toward full protocol generality. These extensions are not required for bootstrapping — the phased launch strategy above is sufficient to capture contributions, build the Contribution Ledger, and enable QP Rewards attribution from day one. However, the architectural separation of the Three-Plane Architecture (below) is designed from the outset to support these extensions without structural refactoring:

- **Multi-substrate persistence**: The Contribution Ledger, Authorization Ledger, and Settlement Ledger (when activated) replicate across multiple independent persistence substrates — including distributed ledger systems (Hedera HCS, Ethereum, Solana), enterprise cloud infrastructure, sovereign registries, and hybrid configurations — through a Persistence Adapter interface that abstracts substrate-specific operations behind a common write/query/verify API. No single substrate is required; contributors and Accelerators select persistence strategies appropriate to their jurisdictional, compliance,

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

and trust requirements. The current implementation persists to cloud infrastructure; ledger-anchored persistence activates as substrate integrations mature.

- **Identity abstraction**: Contributor identity in the current implementation is managed through the Catalyst application's account system. In subsequent phases, the identity layer generalizes to support Quantum Privacy Cells (QPCs), W3C Verifiable Credentials, decentralized identifiers (DIDs), zero-knowledge proofs, institutional identity frameworks, and federated authentication systems — individually or in combination. The core invariant is that contribution attribution must be cryptographically verifiable and privacy-preserving; the specific identity primitives implementing this invariant are not architecturally constrained.

- **Institutional and ambient capture modes**: Beyond the active and the directed capture channels deployed in v1.0 and v1.1, the architecture supports Institutional Mode (enterprise-authorized retrospective processing of institutional data stores to reconstruct contribution history at scale) and Ambient Mode (privacy-preserving monitoring of authorized sources with per-contributor opt-in). These modes activate under explicit governance controls and human approval requirements, as specified in the Five Signal Input Mode Architecture described in Appendix B.

Automation Pipelines vs. Agent Capabilities

Not everything in the agentic architecture requires an agent. The Catalyst implementation draws a precise boundary between deterministic automation pipelines and genuine agent capabilities, and this distinction shapes implementation sequencing, cost modeling, and trust.

Automation pipelines handle capabilities where the action is predetermined and the only question is whether a candidate meets the threshold: contribution linking (matching on same organization, same people, temporal proximity, contribution type progression), objective-to-contribution alignment scoring, dormant chain detection (time thresholds by contribution type), evidence strength classification, anomaly and duplicate detection, reputation computation, objective progress tracking, and XP/level/badge computation. These produce scored candidates for human approval, can be evaluated with precision/recall metrics, and can be deployed with high confidence.

Agent capabilities handle genuine ambiguity where the right action depends on contextual judgment: signal interpretation (is an incoming email a new contribution, evidence for an existing one, a follow-up in a chain, or noise?), conversational context resolution ("the MOU came through for that fintech deal" — which chain?), nudge composition (when, who, how, and whether to nudge a dormant chain), briefing generation (what does this admin need to know before their meeting?), introduction suggestion (who should meet whom to unblock this objective?), and personalized opportunity recommendation. These require LLM orchestration and the Data Plane Log for calibration.

Some capabilities are hybrid: dormant chain detection is automation (time threshold exceeded, surface the dormant chain), but the response — contextual judgment about when, who, how, and whether to nudge — is an agent decision. The implementation priority follows from this distinction: automation pipelines first, agent capabilities where they create the most value. Pipelines are cheaper, faster to build, and easier to evaluate. Agent capabilities add value where ambiguity and contextual judgment materially improve outcomes.

Three-Plane Architecture

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Data Plane:** The factual record layer and home of all intelligence. Contains the Contribution Ingestor (conversational LLM extraction pipeline), the Reputation Engine (pure computation — DFS graph traversal, outcome confidence, reputation signals, badges), the Proximity Engine (contributor-to-objective relevance scoring), and the Contribution Ledger (immutable, governance-grade store of Contribution VCs).
- **Control Plane (QPC Governance):** The authorization boundary. Every consequential action flows through the Control Plane for policy validation and human approval before execution. In v1.0, the human admin serves as the Control Plane — every linking decision, classification judgment, and objective update is made by a person. The Authorization Server, Command Agent, and Person Approval Workflow activate as the agentic architecture matures.
- **Management Plane:** Programs, Accelerators, Objectives, the Organization Directory, and Policies. Configures both Data Plane and Control Plane.

This separation ensures that Catalyst makes no economic claims; PNX governance never dictates what gets recorded. Settlement is based on verifiable contribution facts from the Contribution Ledger, not on agent decisions, logs, or internal operational state. Separate books, separate governance, separate timing.

The Three-Plane Architecture maps to a three-ledger data model that enforces governance separation across the full lifecycle:

- **Contribution Ledger** (Data Plane) records factual attribution claims;
- **Authorization Ledger** (Control Plane) records policy decisions, approvals, and governance actions; and
- **Settlement Ledger** (activated under PNX governance) records economic valuations and token attribution.

Each ledger may persist to different substrates with different replication strategies, ensuring that no single system failure, governance compromise, or substrate limitation affects the integrity of the other two. In the initial SaaS embodiment, these ledgers share a common persistence layer; as multi-substrate persistence is enabled, they may be split across or replicated to independent substrates appropriate to their governance requirements.

Production Infrastructure

Validated in Prototype, Activating in Subsequent Releases

The QPN Catalyst prototype validates the full product architecture with working implementations of capabilities that activate as contributor density justifies them. These are not speculative features — they are built, tested, and deliberately sequenced:

- **Gamification engine:** 10 levels, 24 badges, dual XP streams, streak multipliers, daily caps. The adoption bridge that drives Days 1–90 habit formation for new contributors scaling beyond the founding cohort (see §7.5).
- **Reputation engine:** Pure computation module — DFS graph traversal, 5-tier outcome confidence, 7 reputation signals, 6 reputation badges (Chain Closer, Chain Catalyst, Objective Achiever, Cross Pollinator, Strong Evidence, Network Builder). Answers “did my work matter?” by distinguishing activity from impact. No LLM dependency — deterministic and independently testable. Activates automatically when structured contribution linking ships.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Objectives and proximity personalization:** Admin-managed structured intent with goal rules and contributor-to-objective relevance scoring. Provides scalable "what should I do next?" guidance, replacing linear admin direction with a data-driven mechanism. Activates when contribution volume supports meaningful proximity computation.
- **Chain graphs and structured linking:** Interactive graph visualizations with typed directed edges (follow_up, outcome_of, enabled_by, duplicate_of). Makes contribution chains visible and traceable — showing how introductions led to meetings, meetings to MOUs, and MOUs to deployed networks.
- **Network Impact profile:** Impact signal cards, chain participation panels, connection strength, and AI-generated narrative summaries. Transforms the contributor profile from factual counts into a shareable portfolio that answers "what have I built and what did it achieve?"
- **Analytics dashboard:** Aggregate statistics, time-series, and distribution charts for program managers and accelerator administrators.

These capabilities are fully implemented in the prototype and deliberately sequenced for activation when the network reaches the density where each becomes meaningful. The code remains in the codebase; features light up when their dependencies ship.

Multi-Surface Distribution

The API-first architecture extracts all business logic into a standalone Catalyst API Service, enabling distribution surfaces beyond the web application and email. The core insight: most contributions happen outside Catalyst — in email introductions, calendar meetings, follow-up threads, and partnership discussions. The biggest risk to the Contribution Ledger is not extraction errors — it is contributions that are never recorded because the contributor didn't think to record. Moving capture to where work happens reduces this risk.

Planned distribution surfaces include a browser extension (Catalyst Assistant) that detects contributions where they happen and prompts in-context recording, AI desktop plugins for Claude and ChatGPT enabling batch recording and portfolio generation, and future MCP-based integrations. These extend contribution capture into the professional tools contributors already use while maintaining a single canonical Contribution Ledger.

Agentic Evolution

The Catalyst application's architecture is designed as the foundation for a governed agent evolution. Today Catalyst is an intelligent recorder — the human decides to record, the LLM extracts and structures, the contribution lands in the Ledger. The agentic evolution transforms Catalyst into an active network participant that detects opportunities, proposes actions, and orchestrates follow-ups — with the human providing approval at key decision points rather than driving every step.

Three structural problems motivate this shift: silent data loss (contributions that never get recorded because multi-touchpoint chains happen over weeks and each requires someone to remember), retrospective-only intelligence (the reputation engine computes chain depth and objective alignment, but only after the data exists — nobody watches live chains to detect when they're going cold), and linear admin scaling (objective linking, evidence verification, and analytics interpretation all require a human admin whose workload grows proportionally with the network).

The progression moves through conversational context persistence, chain nudging (detecting dormant chains and composing contextual follow-ups), directed input via email and

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

messaging channels, evidence orchestration, admin automation, ambient detection with per-contributor opt-in, personal agent capabilities, and full Proof-of-Trust governance integration with Trust Block VC issuance and credential-based settlement.

The governed agent loop (Sense → Interpret → Propose → Authorize → Execute → Verify → Learn) ensures intelligence is unbounded while execution is bounded by human approval and QPC governance.

The agentic evolution path described above is specific to the QPN Catalyst application, but the underlying pattern — a governed agent operating within a Proof-of-Trust authorization boundary, with human approval at consequential decision points — generalizes to any contribution capture and attribution system operating within the QPN/PNX architecture. In alternative embodiments, the governed agent loop may be implemented through enterprise workflow automation, third-party AI orchestration platforms, or sovereign coordination systems, provided the Control Plane governance invariant is maintained: no economic claim is made, and no settlement action is taken, without verifiable human authorization or Proof-of-Trust-validated policy compliance.

Meta-Protocol Architecture: Implementation-Agnostic, Century-Scale Coordination

The QPN Catalyst and the broader Privacy Network Exchange are not defined by any single application, ledger, identity system, or execution environment. They constitute an implementation-agnostic coordination protocol designed to persist across successive generations of technology. Where most platforms are tightly coupled to their initial implementation choices — specific blockchains, databases, identity providers, or application architectures — the QPN/PNX architecture deliberately separates invariant protocol properties (contribution attribution, Proof-of-Trust governance, privacy-preserving identity, and settlement linkage) from the mutable systems that implement them.

This decoupling enables continuous migration across substrates, identity frameworks, AI systems, and infrastructure layers without breaking economic continuity or invalidating historical contribution records. The Contribution, Authorization, and Settlement Ledgers may be instantiated on different substrates, replicated across multiple systems, or evolved independently over time — while maintaining cryptographic and governance continuity through the Unified Trust Model. Catalyst is therefore not merely a product but a meta-protocol coordination layer that can attach to any application, enterprise system, or network, capturing and attributing value without requiring those systems to be replaced or modified.

This design is essential for an ecosystem intended to persist and compound over centuries rather than decades. It ensures resilience to technological obsolescence, regulatory evolution, and shifting market structures, while preserving the integrity of contribution attribution and economic rights across time. The result is a system that compounds rather than resets with each technological wave — allowing the network, its participants, and their accumulated contributions to survive and strengthen through successive cycles of innovation.

7.7 The Participant Experience and Economic Interface

The preceding sections describe how the Catalyst captures and attributes contributions. This section describes what those contributions are worth, why timing matters, and why rational participants act immediately.

From Submission to Value: The Attribution Chain

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

A submission to the Catalyst Network creates no ownership interest, economic right, or thing of value. This is not a legal technicality — it reflects the fundamental architecture of the system. Value in the QPN ecosystem is not created by recording an action; it is created when that action produces a real-world outcome, and the participant's role in producing that outcome can be verified.

The path from submission to value runs through a chain with four links, each of which must be completed before QP Rewards can be allocated.

The first link is a causal connection. Individual contributions must be linked into contribution graphs that reach Activation or Cascade Milestones — enterprise commitments, partnership agreements, production deployments, public announcements, or other events that advance the ecosystem from aspiration to reality. An introduction that leads to a Tier 1 Anchor commitment sits at the root of a cascade graph worth billions. An introduction that goes nowhere remains in the Contribution Ledger as conditional attribution — preserved, timestamped, and available for future chain-linkage if downstream events eventually complete the connection, but generating no QP Rewards until they do. A submission in isolation is evidence, not an entitlement.

The second link is real-world value creation. Contribution graphs must connect to outcomes that generate measurable economic value within the Privacy Network Exchange — the formation of Quantum Privacy Resources, Exchange Networks, Resource Pools, or settlement-generating deployments. Not all valuable contributions require institutional participation: public commitments by individuals, enterprises, organizations, or government entities are inherently valuable under the Strategic and Publicity Premiums, and may enable inferred linkages into the contribution graphs that implement those commitments across the committing entity's broader ecosystem. Personal evangelism — advocating through professional networks, public platforms, and communities — is independently valuable, weighted by the advocate's credibility, domain expertise, reputation, organizational affiliations, and the breadth and influence of their relationships. An individual whose public endorsement shifts perception across an industry can anchor contribution graphs worth as much as any enterprise commitment.

The third link is time. The ecosystem is in its earliest stages, and the outcomes that generate QP Rewards — settlement-generating Exchange Networks, operating Resource Pools, production deployments — take time to build. There is no guarantee that any particular contribution, contribution graph, or Activation Milestone will ultimately produce QP Rewards. The Deferred Activation model — where contributions are recorded now but value is allocated later — exists precisely because the system needs time to determine which contributions actually mattered. This delay also serves a protective function: it ensures that every allocation can be verified for compliance with employment agreements, fiduciary obligations, and applicable regulatory restrictions before any value is transferred, shielding participants from inadvertent conflicts they may not have anticipated at the time of contribution.

The fourth link is compliance verification. All contribution graphs are reviewed by the Privacy-Preserving Compliance Service before allocations are finalized, verifying compliance with the Unified Trust Model, applicable law, and the ethical and public-benefit requirements of the Participation Agreement. This review operates at the level of individual allocations, not entire contribution graphs — it is not all or nothing. A participant whose contribution graph spans both personal advocacy and professional activities may find that allocations related to their professional role are reclassified as Restricted Derivative Rights (RDRs) and redirected to public-benefit entities, while allocations arising from personal advocacy within the same graph remain fully available. Every person and organization has been granted a QPC Option

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

that always entitles them to participate through personal advocacy — a right protected under constitutional, labor, and employment law — even if allocations directly related to professional, governmental, or fiduciary roles are restricted or redirected. The system is designed to maximize the scope of legitimate participation, not to create barriers that exclude people from the opportunity.

Only when all four links are complete — causal connection established, real-world value created, sufficient time elapsed, and compliance verified — can QP Rewards be allocated. Until then, submissions accumulate as evidence in the Contribution Ledger: timestamped, preserved, and waiting for the chain to complete.

All allocation determinations are governed by the **QP Rewards Allocation Model**, a systematic framework guided by the Unified Trust Model Premiums — including the Strategic, Timing, Value, Cascade, and Publicity Premiums — that evaluates contributions based on verified causal linkage, relative timing, independent corroboration, and downstream impact. The Managers of Quantum Privacy LLC retain sole and absolute discretion over the design, calibration, and interpretation of the Allocation Model, but individual allocations are determined by the model's application to the contribution graph, not by ad hoc managerial decisions.

This structural reality — that value requires a complete chain from submission through verified real-world outcomes — is what makes early participation so consequential. The contributions that complete the earliest chains, triggering the first Cascade Milestones and unlocking the first settlement flows, sit at the highest point on the Premium Multiple curve. The next section explains why.

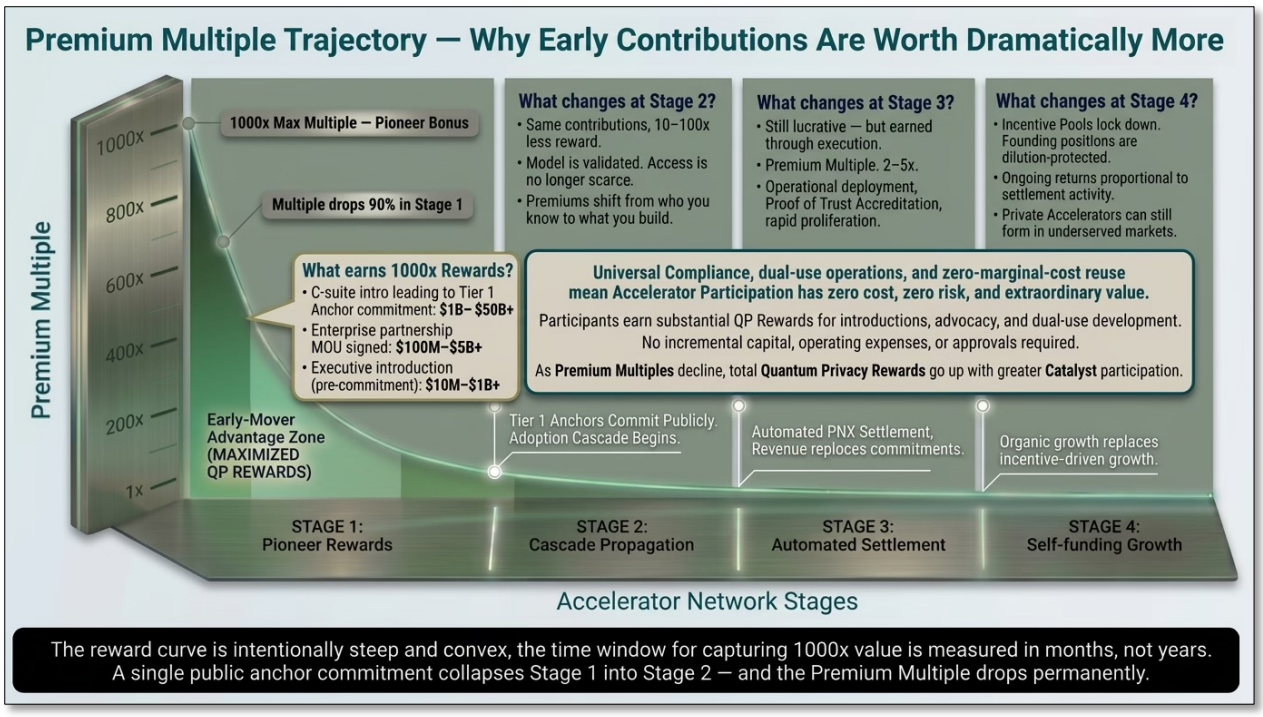
Quantum Privacy Rewards and the Premium Multiple

Every contribution captured by the Catalyst — an introduction, an enterprise engagement, a technical component, an advocacy effort — accumulates as a verified record within the contributor’s Quantum Privacy Cell. When PNX settlement activates, these records become the basis for Quantum Privacy Rewards: economic allocations proportional to each contributor’s verified causal role in enabling settlement value.

The value of any given contribution is not fixed at the time of recording. It is determined retrospectively by the downstream settlement value that the contribution helped enable, weighted by the five Launch Premiums (Strategic, Timing, Value, Cascade, and Publicity) and moderated by the Proportionality and Balance Premiums that govern long-run fairness and ecosystem health. The Premium Multiple is the ratio of QP Rewards earned per unit of contribution effort at a given stage compared to the base-level reward earned for equivalent effort once the network reaches steady state. A Premium Multiple of 100x means the same type and quality of contribution earns 100 times the steady-state reward.

The Premium Multiple is not a single number — it is a distribution that is heavily front-loaded within each stage. The very first contribution that triggers a Tier 1 Anchor commitment earns at the top of the range; the same type of contribution after several anchors have committed earns at the bottom, because the Launch Premiums have compressed and the contribution is less scarce.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved



Why Early Premium Multiples Translate to Trillions

The massive dollar magnitudes associated with early Premium Multiples arise from a specific mechanism: cascade value capture. Early contributions sit at the root of cascade graphs that propagate into enormous downstream settlement value, and the contributor earns a share of that entire downstream value through the contribution graph attribution mechanism.

The causal chain operates as follows: an introduction triggers an anchor commitment. That commitment triggers awareness, validation, and competitive dynamics across peer enterprises. Each peer's participation triggers its own ecosystem of customers, vendors, and partners. Settlement density compounds across all of them. Exchange Tokens flow back through the contribution graph proportional to verified causal contribution. The contributor's QP Rewards are a fraction of a massive total — not a large fraction of a small total.

As cascades propagate, each incremental contribution triggers less additional cascade value, because most of the downstream ecosystem is already in motion. This is the second mechanism driving the Premium Multiple curve downward — not just Launch Premium compression (scarcity), but declining marginal cascade value per contribution. Both mechanisms push in the same direction and compound multiplicatively, which is why the Premium Multiple curve is steeply convex.

Four Stages of the Accelerator Network

The Premium Multiple trajectory maps to four structural stages of ecosystem maturation. These stages are milestone-driven, not calendar-driven — transitions occur when specific structural events are achieved, not on predetermined dates.

Stage 1: Pioneer Rewards. Tier 1 Accelerator Anchors are being recruited. First MOUs and strategic commitments are forming. No cascade yet triggered. Premium Multiple: 100–1,000x+. Contributions that trigger anchor commitments sit atop cascade graphs worth trillions. The contributor pool consists of dozens to hundreds of individuals. Three architectural properties make participation genuinely zero-cost and zero-risk: dual-use operations (contributions leverage activities participants are already doing), zero-marginal-cost reuse (contributed resources are reused without additional cost), and Universal

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Compliance (the QPC architecture requires no employer disclosure, no regulatory approvals, and no public commitment).

Stage 2: Cascade Propagation. One or more Adoption Cascades have been triggered. First PNX settlement events recorded. Because cascades are horizontal and cross-propagating, triggering any one rapidly propagates across all verticals and geographies. Premium Multiple: 10–50x. The model is validated, access is no longer scarce, and Premiums shift from who you know to what you build. The contributor pool expands to hundreds or thousands of individuals and dozens of enterprises or more.

Stage 3: Automated Settlement. Multiple cascades are converging. Automated settlement via the QP Token Platform is operational. Measurable settlement density across sectors. Premium Multiple: 2–5x. Returns are still above steady-state but earned through operational execution — deployment, governance, Proof-of-Trust accreditation, and scaling.

Stage 4: Self-Funding Growth. The network is growing rapidly and self-funding. Founding positions are dilution-protected once Accelerator Incentive Pools lock down. Lock-down occurs when the Exchange Networks and Resource Pools incubated by an Accelerator have reached sufficient scale and Monetization Uplift Multiple (MUM) that new participants have a strong economic incentive to join through Accelerator Participation Pools — earning Exchange Tokens from the 80% Participant Pool through ongoing operational contributions — without requiring Accelerator Token incentives from the 20% Incentive & Investment Pool. Premium Multiple: 1x (base level). The ecosystem remains open and rewarding; it is the founding-phase incentive layer that closes, not the settlement economics.

Across these four stages, the nature of what earns disproportionate QP Rewards shifts progressively: from who you know (introductions and access in Stage 1), to what you build (operational contributions in Stage 2), to how well you execute (deployment excellence in Stage 3), to proportional participation (settlement-linked returns in Stage 4). This progression is not a policy choice — it is an emergent consequence of the Launch Premiums compressing as the ecosystem matures.

Total QP Rewards Increase as Premium Multiples Decline

A natural concern is that declining Premium Multiples mean declining rewards. The opposite is true. As the Premium Multiple declines from 1,000x to 1x, the total pool of QP Rewards flowing through the system increases dramatically — because the events that compress the Premium Multiple (anchor commitments, cascade propagation, settlement activation) simultaneously expand Catalyst participation and settlement density. The Premium Multiple is a ratio: QP Rewards per unit of contribution effort relative to steady-state. When the Multiple drops from 1,000x to 10x, the per-contribution reward has declined relative to the peak — but the total number of contributions, the total settlement volume, and the total QP Rewards distributed across all participants have all increased by orders of magnitude.

Moreover, the nature of later-stage contributions shifts in a way that makes rewards feel more immediate and certain. In Stage 1, contributions are speculative bets on cascade formation — an introduction may or may not lead to an anchor commitment, and settlement may be months or years away. By Stage 3, the ecosystem has momentum: contributions are tightly linked to specific solutions with near-term settlement activity, and a deep pool of existing QP Resources is already available for zero-marginal-cost reuse. This means later-stage contributors can see a much clearer path from their contribution to actual Exchange Token settlement — reducing uncertainty even as the per-contribution Premium Multiple is lower. The tradeoff between early and late participation is therefore not simply "high reward vs. low

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

reward" — it is "high potential magnitude with high uncertainty and long time-to-settlement" versus "lower magnitude with higher certainty and near-term realization."

This is why participation at any stage remains attractive: even at a 2–5x Multiple in Stage 3, a participant earns 2–5 times the steady-state reward from a much larger and faster-growing settlement base, with a clearer line of sight to when and how that reward materializes. The absolute dollar value of Stage 3 contributions can still be substantial — just not the billions or tens of billions available to those who triggered the cascades in the first place.

Why Immediate Participation Is the Dominant Strategy

The structural conditions described above create a participation calculus where delay is the primary source of value destruction. Five properties combine to make immediate participation the dominant strategy for rational actors:

First, participation has negligible downside. Dual-use operations, zero-marginal-cost reuse, and Universal Compliance mean contributions require no incremental capital, no operating expenses, and no employer or regulatory approvals. Participants can contribute through their existing professional activities without changing how they work.

Second, early allocation is durable. Contributions captured now are recorded permanently in the Contribution Ledger and attributed retrospectively when settlement activates. A position established at Stage 1 Premium Multiples cannot be replicated later at lower multiples — the contribution graph locks the contributor's position at the time of recording, not at the time of settlement.

Third, participation increases the probability of network success. Each additional participant expands the contribution graph, increases the density of Exchange Networks and Resource Pools, and accelerates the cascade dynamics that drive settlement activation. Participation is self-reinforcing.

Fourth, adoption cascades are horizontal and cross-propagating. Triggering any one of the four cascades (Enterprise, Grassroots, Investment, Sovereign) rapidly propagates across all sectors and inevitably triggers the remaining three. The transition from Stage 1 to Stage 2 can occur in days once a trigger fires — and when it does, the Premium Multiple drops permanently.

Fifth, the laggard penalty is severe and asymmetric. For enterprises, the penalty is approximately 85–90% — driven by lost trust taxonomy anchoring, routing centrality, and Incentive Pool allocation. For individuals making introductions and providing initial access, the penalty approaches 95–99%+ once cascades are triggered, because those contributions become abundant rather than scarce. The window for maximum individual QP Rewards from relationship-driven contributions is measured in weeks, not months.

The Contributor-Centric Narrative appendix provides quantified reward trajectories by contribution type across all four stages, detailed Premium Multiple derivations, and illustrative dollar ranges grounded in the 80/20 Accelerator waterfall applied to P50 ecosystem magnitude estimates.

7.8 The Milliman-Anchored Production Environment

Parallel development is possible from day one because Milliman's existing infrastructure provides a fully functional development and deployment substrate for all six implementation layers. Key assets:

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Databricks on Azure:** Milliman's production Databricks environment supports governed analytics, data linkage, tokenization, and DeltaShare-based cross-organizational data exchange. DeltaShares already implement the governed data-sharing pattern that the PNX generalizes. Unity Catalog provides fine-grained access controls, column-level security, row filters, and audit logging that serve as Stage 1 delegated governance.
- **Azure, AWS, GCP Multi-Cloud:** Hundreds of millions of dollars in committed cloud infrastructure spend across all three major hyperscalers means that every cloud-native component can be developed, tested, and deployed within production-grade environments without provisioning new infrastructure.
- **Population-Scale Data Assets:** Thousands of enterprise data sources and long-standing data-sharing agreements across healthcare, insurance, financial services, and government provide the actual governed data against which Resource Publishing components are developed. EHR adapters can be tested against real clinical data; financial data bridges against real claims and actuarial data — all under Milliman's existing data use agreements.
- **Governance & Compliance Controls:** HIPAA, SOC 2, and financial services compliance frameworks already in force mean that components developed and deployed within Milliman's environment inherit production-grade compliance from day one. These controls are configurable through Unity Catalog, Entra ID, and other enterprise governance platforms — not hardcoded.
- **ICON Plc Clinical Research Network:** ICON's 40,000 employees across 50+ countries, signed teaming agreement, and relationships with every major global pharmaceutical company provide the vertical market depth for healthcare-specific Resource Publishing.

7.9 Parallel Development Tracks

The development proceeds on three parallel tracks that compress time from investment to revenue:

- **Track A — Core Runtime and Foundations:** Accelerator Catalyst Layer, Core Runtime Layer components (QPC Lifecycle, EasyAccess, Exchange Network Runtime, Quantum Rating System), and Cryptographic & Identity Layer. Requires the most specialized expertise and architectural coordination, but its deliverables can be validated inside Milliman's containment.
- **Track B — Resource Publishing and Governance:** All Resource Publishing Layer components and the Governance & Compliance Layer. Immediately developable against Milliman's existing infrastructure. Each vendor API integration (Salesforce CRM, Epic EHR, Snowflake, Azure ML, etc.) can be independently built, tested, and validated against live data in the interim PNX environment.
- **Track C — Exchange, Content & Liquidity:** Personalized Exchange Engine, AI Content Engine, and Token Platform Bridge. Exchange and content engines depend on Resource Publishing components being available. Token Platform activation (the only explicitly sequenced component) proceeds on Track B timing.

By the time Core Runtime components reach controlled beta, multiple Resource Publishing components are already operational and generating settlement — dramatically compressing the time from investment to revenue.

7.10 Core Team Funding Pathways

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

The irreducible core team — architects, cryptographic engineers, protocol designers, and program managers — is 15–25 people but high-caliber. Multiple funding mechanisms apply simultaneously:

- **Donated Staff:** Enterprises, technology vendors, consulting firms, and systems integrators assign employees as in-kind contributions. A hyperscaler that seconds two senior architects, a consulting firm that assigns three cryptographic engineers, and an identity vendor that donates a product manager can collectively fund a significant portion of the core team at zero cash cost.
- **Investment in EP3 and/or Accelerators:** Venture capital, corporate venture, strategic investors, and sovereign wealth funds invest directly in EP3 Networks, WebShield, or specific Accelerator entities. These investments fund core team operations while giving investors equity exposure to the settlement economics.
- **Philanthropic Contributions:** The QPN's privacy-preserving, person-centered architecture aligns with the missions of major technology philanthropy, digital rights organizations, and public-interest foundations.
- **Professional Services Fees:** Core team members provide architectural advisory, integration design, and compliance assessment services to enterprises seeking to connect to the PNX. These services generate revenue that funds ongoing operations while simultaneously advancing component development.
- **Grants and Government Funding:** The Lokahi Healthcare Accelerator operates within a statewide initiative supported by over $1 billion in federal, state, and CMS innovation funding. Grant mechanisms — CMS innovation grants, DARPA/NSF post-quantum cryptography programs, NIH data interoperability grants, DOE privacy-preserving computation grants — directly fund component development.
- **Enterprise Sponsorship for First-Mover Advantage:** Enterprises that understand the cascading adoption dynamics and recognize that foundational PNX positioning will pay massive dividends as settlement volume scales will compete for the core team's attention. The core team's bandwidth is inherently scarce — 15–25 people making foundational architectural decisions, with hundreds of potential enterprise sponsors, technology vendors, and investors who want their platforms prioritized. This scarcity creates pricing power. The question is not whether sufficient resources exist to fund the core team for 18 months, but how to manage the competitive demand from enterprises and investors who recognize that early participation is the most capital-efficient investment available.

7.11 Implementation Phases

Phase 0: Earning Prelaunch Rewards

Phase 0 is the period before Exchange Token settlement goes live — before all Capture Tools are fully operational and before the network reaches the density required for automated rewards. It is also the period when Prelaunch Rewards are at their most valuable: Launch Premiums are highest for the earliest participants, XP accumulation begins from the first contribution, and the attribution records built now form the foundation of every downstream Quantum Privacy Rewards calculation at settlement.

Every contributor who captures ecosystem activity during Phase 0 builds an XP-visible record that directly feeds their Quantum Privacy Rewards allocation at settlement. The QPN Catalyst application (WebVector) provides four Active Mode input methods:

- **Voice** (browser speech recognition with real-time transcription)

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Paste** (clipboard text for LLM extraction)
- **Upload** (PDF/DOCX/TXT with server-side extraction and auto-evidence)
- **Manual** (direct form entry)

The entire recording flow can be completed in under 60 seconds. Email intake extends capture to Directed Mode (CC qpncatalyst@inbound.webshield.io on any email). Evangelized Mode operates from Phase 0 onward through EasyAccess Links and public advocacy.

Contributors who capture their ecosystem activity now are not doing so on faith: every record is cryptographically signed, tamper-evident, and protocol-enforced. The XP layer (§7.5) provides a real-time visible signal that activity is being recorded and valued while settlement infrastructure matures. The Contribution Receipt provides immediate confirmation that each record has been stored. And the Attribution Durability guarantees (§A.9) ensure that no record is lost regardless of how the technical infrastructure evolves between capture and payment.

The Three-Phase Evolution Arc: Governed → Auditable → Intelligent

The Catalyst's implementation follows a deliberate three-phase maturity arc described by three words: Governed, Auditable, Intelligent.

"***If you helped build it, you should own a piece of it***." — the founding promise of the Deferred Activation architecture — is what the three-phase evolution is designed to deliver. Contributors who capture their ecosystem-building activity in Phase 0 accumulate verifiable, cryptographically-signed attribution records that mature into ownership stakes as the network reaches settlement readiness. Phase 1–2 builds the auditability layer that makes deferred ownership trustworthy. Phase 3–4 delivers the intelligence to make ownership allocation precise. Contributors who start capturing in Phase 0 are rewarded later — and at higher accuracy — than would have been possible had rewards been required in real time.

The implementation roadmap progresses through five phases. Full phase specifications are in Appendix A.

The Catalyst application's agentic evolution roadmap maps to the Launch Phases as follows:

- Catalyst Phases 0–1 (conversational context, chain nudging) correspond to Launch Phases 1–2.
- Catalyst Phase 2 (Directed input via email and Slack, implementing CommVector and MessageVector) corresponds to Launch Phase 2.
- Catalyst Phases 3–6 (evidence orchestration, admin automation, ambient detection, personal agent) correspond to Launch Phases 3–4.
- Catalyst Phase 7 (full Proof-of-Trust governance integration) corresponds to Launch Phase 4 governance completion.
- Catalyst Phase 8 (Institutional graph densification) implements the "Enterprise graph densification through Private Accelerator dual-use integration" described in Launch Phase 4.
- Catalyst Phase 9 (Evangelized distribution and cascade attribution) operates continuously from Launch Phase 0 onward, scaling with EasyAccess infrastructure maturity.

Launch Phases

Phase	Key Deliverables & Timing

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Phase 0 — Interim Manager-Hosted Persistence (Immediate)	Cloud-hosted contribution record storage (AWS/Azure/GCP) operated by Quantum Privacy LLC or Managing Members. EP3 Fellows as initial cohort. QPCPA §3.3(c) and §3.4 provide legal authorization — no new agreements required. All records classified as Confidential Information under Exhibit B trade-secret protections. Deployable within days via cloud-service configuration, not software development.
Phase 1 — Foundation (Immediate)	Manual attribution tool ("Bounty Hunter") web interface. CLI-based CodeVector alpha. EP3 Contribution Context published at public endpoint. Persistence Adapter interface defined. LocalArchiveAdapter and ManagerHostedAdapter implemented. Persistence Router with Write-Primary-Plus-Backup default (local + Phase 0 cloud). Basic PRIVATE/MANAGER visibility tiers and cross-verification via encrypted messaging.
Phase 2 — Automation & Collaboration (Near-Term)	Gemini/Outlook sidecar extension. Deal Flow dashboard. Retrospective Archaeology with semantic evaluation. VS Code extension. HederaAdapter implemented. PARTICIPANT and VERIFIED_PUBLIC visibility tiers. Manager-posted bounties. Capability signaling. Basic Graph Coordination Dashboard.
Phase 3 — Intelligence & Coordination (Medium-Term)	Desktop add-ins (Outlook, VS Code, JetBrains). Bulk retrospective processing. Enterprise and cloud adapters (PostgreSQL, S3). Write-N-of-M strategy. Global Graph Assembly Engine deployed with fragment linking and retrospective chain reconstruction. AI-assisted dispute resolution. Algorithmic coordination matching. Participant-posted bounties with negotiated reward sharing.
Phase 4 — Full Ecosystem Intelligence (Longer-Term)	Server-side enterprise API for the AI Evaluation Pipeline. EasyAccess IdP integration. Enterprise graph densification through Private Accelerator dual-use integration. Cross-Accelerator graph synthesis through EP3 Proof-of-Trust. Sovereign data store adapters. Continuous substrate expansion and monotonically increasing resilience.

Each phase also represents a distinct maturity level in how the system operates:

- **Governed (Phase 0–1):** Contribution capture, attribution, and rewards allocation are managed through administrative processes — Manager-reviewed submissions, manual Objective Linking, structured web forms, and the VoiceVector app. The system is legally authorized, cryptographically sound, and operationally functional, but human judgment remains central to classification and validation. This phase establishes the legal and relational trust foundation on which subsequent automation is built.
- **Auditable (Phase 2–3):** Automated classification, cross-verification, and graph assembly replace or supplement manual processes. Every decision made by the system is logged, explainable, and auditable against the canonical EP3 Contribution Context. The AI Evaluation Pipeline, the Cross-Verification Protocol, and the Global Graph Assembly Engine become primary — human Manager review shifts from gatekeeping to exception handling. Attribution records accumulate sufficient density to support statistical validation of classification accuracy.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Intelligent (Phase 4+):** The system develops proactive intelligence — the Contributor Context Profile enables cross-session cascade detection, the Graph Coordination Dashboard surfaces collaboration opportunities, the Nearby Opportunities feed anticipates contributor needs before they arise, and the AI-Assisted Dispute Resolution system resolves attribution conflicts without human escalation. The network is self-improving: graph density increases classification accuracy, which increases reward precision, which increases contributor quality, which increases graph density.

Phase 0: Detailed Specification

- **Legal Foundation.** Phase 0 requires no new legal agreements. The existing Quantum Privacy Cell Participation Agreement (QPCPA) provides comprehensive authorization and protection. Section 3.3(c) explicitly contemplates "a phased migration to privacy-preserving recordkeeping systems" from initial manual processes. Section 3.4 authorizes participant reliance on "manual or administrative mechanisms or practices established by the Quantum Privacy LLC or its Managers for the creation, maintenance, or verification of records or allocations." All Contribution Records stored in the Phase 0 layer are classified as Confidential Information and trade secrets of Quantum Privacy LLC under Exhibit B (Confidentiality and Non-Disclosure Terms) and Section 7 (Confidential Existence of QPCs) of the QPCPA, and are subject to the full protections described in Section 10 of this document.
- **Access Authorization**. The Managers and Executive Director may access, review, and audit Catalyst Intake Records solely for five enumerated Permitted Audit Purposes:
  (1) verifying the accuracy and completeness of Contribution Records and attribution metadata;
  (2) resolving disputes concerning the attribution, timing, or classification of Contribution Records;
  (3) auditing the integrity and performance of the Catalyst AI Evaluation Pipeline and related automated systems;
  (4) investigating potential fraud, data corruption, or system malfunction affecting the Catalyst Contribution Ledger; and
  (5) ensuring compliance with the Unified Trust Model, Proof-of-Trust protocols, and applicable law.

  These purpose limitations apply to all Catalyst Intake Records regardless of contributor visibility settings. **Contributors who set visibility to MANAGER tier grant additional authorization beyond the Permitted Audit Purposes:** designated Accelerator Managers — including Quantum Privacy LLC, WebShield Inc., and EP3 Foundation — may decrypt, link, and analyze their Contribution Records for the additional purpose of facilitating the extension of contribution graphs to reach Activation or Cascade Milestones, and to facilitate ecosystem development.
- **Contribution Verification and Participant Engagement.** For activated participants (who have executed the QPCPA), Managers can reach out directly to verify contributions, confirm chain linkages, and validate attribution — this falls within the 'verifying accuracy' and 'resolving attribution disputes' Permitted Audit Purposes. The participant's QPC Cell Classification under Section 14.3 of the Participation Agreement governs the scope of disclosure in these interactions. For DORMANT QPCs (pre-activation), direct outreach raises a design constraint: contacting the submitter would reveal that the system has their submissions, which is a disclosure the system is designed to avoid in Silent Mode.

  The preferred verification mechanisms for pre-activation submissions are:

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

(a) cross-referencing with other participants' independently submitted records to corroborate chains;

(b) using the Acknowledgment and Evidentiary Response Modes, which give submitters a reason to engage and a path to the Catalyst App where they can proactively verify and enrich their submissions; and

(c) encouraging early activation through the Participant Guide and landing page, which converts DORMANT QPCs to activated ones where full verification engagement is authorized.

The design principle is: create pull rather than push. Response Modes, the landing page, and the Participant Guide give submitters reasons to engage, discover the opportunity, and activate — at which point verification becomes a collaborative process between the participant and the Managers.

- **Initial Cohort: EP3 Fellows.** Phase 0 launches with existing EP3 Fellows as the initial contributor population. Fellows are already actively and openly involved in the QPN/PNX ecosystem, currently making introductions, facilitating enterprise engagement, and building technical capabilities. To be eligible to receive Quantum Privacy Rewards, they will execute QPCPAs. Their participation is not subject to the dual-use compliance concerns that the Catalyst's zero-knowledge architecture is designed to address, reducing initial privacy requirements to standard enterprise-grade encryption and access control. Fellows provide informed feedback on classification accuracy, entity-resolution quality, and coordination workflows, directly shaping the production system. As Phase 0 demonstrates operational reliability and feature maturity, additional participants — including dual-use contributors requiring stronger privacy guarantees — are onboarded incrementally with progressively stronger cryptographic controls.
- **Persistence Adapter Compatibility.** Phase 0 is designed for forward compatibility with the Persistence Adapter architecture. All records use the canonical Attribution Record schema with no Phase 0–specific modifications. When the Persistence Adapter interface is implemented in Phase 1, the Phase 0 cloud storage becomes a reference adapter implementation (ManagerHostedAdapter), registered with the Persistence Router alongside the LocalArchiveAdapter — providing immediate two-substrate diversity with zero data migration. Records stored during Phase 0 can be replayed to any subsequent adapter (Hedera, enterprise databases, sovereign stores) through the Router's standard replay mechanism. Phase 0 may persist indefinitely as one substrate in the Router's diversified portfolio, providing Manager-operated, jurisdiction-specific resilience alongside contributor-controlled and decentralized substrates.
- **Operational Procedures.** The operating Manager maintains automated backups following cloud-provider best practices (cross-region replication, point-in-time recovery, versioned object storage). Access is logged with cloud-native audit trails (AWS CloudTrail, Azure Monitor, GCP Audit Logs); all Manager access is traceable and attributable. The audit trail is itself Confidential Information under the QPCPA. Contributors are encouraged to maintain their own .qpn archives as a contributor-controlled backup. In the event of a security incident, the operating Manager follows cloud-provider incident-response protocols and notifies affected contributors. Protective reconstitution authority under QPCPA Section 4.3 may be invoked if contributor records are compromised or if coercive access is attempted.

V1 Learning Goals

V1 is designed as an instrumented experiment, not just a product launch. The primary observation goal is which input modes contributors actually use, and how that usage should

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

shape subsequent investment. Specific learning signals include: email intake versus app-based recording counts (which determines whether to invest in more integrations or in app UI refinement); voice versus paste versus upload versus manual usage within the app (which determines which in-app flow to optimize); whether contributors view their profiles (which determines how much to invest in the portfolio layer); whether contributors ask for progress feedback (which determines when to activate the gamification engine); and whether contributors miss having structured direction (which determines when to add objectives and proximity personalization).

Features that are fully implemented in the prototype but deliberately excluded from V1 — gamification, objectives with proximity personalization, chain graphs, reputation engine, analytics dashboard, AI narrative summaries — are deferred not because they are unfinished, but because the V1 user cohort (approximately five highly motivated insiders) does not need engagement mechanics or strategic direction tools. The code remains in the codebase and activates when contributor density justifies each feature — gamification when new contributors need habit-formation feedback loops, objectives when contribution volume supports meaningful proximity computation, chain graphs when the graph has enough density to be visually informative, and reputation when chain data and objective links provide the inputs the engine requires. This deliberate sequencing ensures that no feature launches before it can deliver value, and that V1 learning goals drive V2 prioritization with empirical data rather than assumptions.

7.12 Revenue Timeline

Under cascading adoption with billions in ecosystem investment, the QPN achieves cash breakeven on its sub-$50M direct cost within 6–9 months — before most components reach GA — because massive parallel engineering capacity drives multiple components to production simultaneously while settlement begins inside trusted containment from day one.

Milestone	Timeline	Monthly Settlement	Cumulative Settled
First Settlement Events	Month 6–9	$20–$100M	$60–$400M
Platform Enrollment	Month 9–12	$100–$500M	$0.5–2B
Revenue Dominance	Month 12–18	$500M–$2B	$4–15B
Global Standard	Month 18–24	$2–$5B+	$20–50B+
Cash Breakeven	Month 6–9	Ops costs covered	<$50M recovered

Under cascading adoption with billions in ecosystem investment, the QPN achieves cash breakeven on its sub-$50M direct cost within 6–9 months — before most components reach GA — because massive parallel engineering capacity drives multiple components to production simultaneously while settlement begins inside trusted containment from day one. No investment in history — in any industry, at any scale, in any era — has combined this degree of capital efficiency with this magnitude of addressable value.

7.13 Investment Structure

The QPN's direct cost of less than $50M catalyzes $10–25B+ in ecosystem investment through the same competitive dynamics that currently drive $100B+ annual AI infrastructure spending. The leverage ratio of 200–500x is a structural consequence of competitive self-interest among enterprises, vendors, and investors who cannot afford to let rivals establish foundational positioning.

Investment Source	Scale	Timeline

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Core Architecture Team (anchor partnerships, grants)	$5–8M	Months 1–18
Founder / Corporate Investment (tech founders, corp. venture)	$1–5B	Months 3–9
Major Tech Vendor Engineering (1.5k–3k engineers, in-kind)	$500M–$1.5B	Months 3–18
Professional Services Firms (client-funded engagements)	$200M–$1B+	Months 1–18+
Sovereign Accelerators (national government funding)	$1–5B+	Months 3–18
Financial Institution Accelerators (bank/insurer self-funded)	$500M–$2B	Months 6–18
Identity & Data Vendor Teams (revenue-share incentive, in-kind)	$100–500M	Months 3–18
Dual-Use & Independent Catalyst Contributors	$0 cash	Months 1–18+
QPN DIRECT COST (Core team + ops)	**<$50M**	**18 months**
TOTAL ECOSYSTEM INVESTMENT (all sources)	**$10–$25B+**	**18 months**
LEVERAGE RATIO (Ecosystem / QPN direct)	**200–500x**	**Competitive**

8. User Stories: Universal Ownership in Practice

In the early stages of ecosystem formation, the most valuable contributions — code, advocacy, introductions, compliance validation — come from high-performing individuals currently employed by major enterprises. These individuals face a structural dilemma:

- **The Incentive Gap:** They want to contribute to the QPN ecosystem to earn early-adopter Quantum Privacy Rewards.
- **The Compliance Block:** They cannot contribute openly without violating employment contracts, violating conflict-of-interest policies, leaking IP, or triggering Data Loss Prevention (DLP) alarms.
- **The Result:** High-value talent remains on the sidelines, and the ecosystem faces a cold-start problem.

The Solution: The Accelerator Catalyst resolves this by separating the verification of value from the transfer of IP, allowing dual-use work to be attributed to the individual's Quantum Privacy Cell without exposing proprietary content to the QPN ecosystem.

The following ten archetypes illustrate how the Catalyst resolves the Dual-Use Dilemma across the full spectrum of contributor types. Each story is a concrete illustration of how contributions are captured, attributed, and rewarded in practice.

8.1 The Executive Introducer (Strategy Consultant / Connector)

As a Strategy Consultant with Fortune 500 C-suite relationships, I want to cryptographically tag my email introductions between Accelerator leadership and target enterprise executives — capturing a hash of the message content and recipient domain without transmitting any email text — so that I establish a verifiable, privacy-preserving record of my role in initiating Anchor relationships, earning Executive Access Quantum Privacy Rewards with Strategic and

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Cascade Premium weighting as each introduction I facilitate triggers downstream enterprise adoption.

8.2 The Internal Champion (Enterprise Employee / VP / Director)

As a VP of Data Engineering at a major cloud platform, I want to record my internal advocacy activities — executive briefings, assessment memos, pilot authorization requests — as contribution milestones within my QPC, without exposing any internal communications outside my employer's network, so that when the enterprise commits and Exchange Token settlement begins, my months of internal championing are attributable and rewarded proportionally to the adoption I enabled.

8.3 The Portfolio Activator (Venture Capital / Private Equity Partner)

As a VC Partner with a portfolio of 40+ companies, I want to systematically introduce portfolio founders and CTOs to Accelerator leadership and track which introductions convert to pilot commitments or resource publishing, so that the cascade my portfolio activation creates — where each portfolio company that joins triggers introductions to their enterprise customers, partners, and board connections — earns compounding Cascade Premium across the full downstream contribution graph.

8.4 The Big 4 Partner (Audit / Advisory / Professional Services)

As an Equity Partner at a Big 4 audit firm with 200+ Global 1000 client relationships, I want to record my advocacy activities that position my firm as a Trust Authority anchor — including client briefings, practice development, and cross-border regulatory engagement — so that when my firm's commitment enables Proof-of-Trust Accreditation across 140+ countries, the Quantum Privacy Rewards reflect both the Strategic Premium of the firm's commitment and the Cascade Premium from downstream client adoption flowing through my contribution graph.

8.5 The Government Champion (Elected Official / Agency Leader / Policy Advisor)

As a state-level policy advisor with relationships across the Governor's office and federal innovation agencies, I want to record my facilitation of governmental engagement with Accelerator leadership — regulatory briefings, interagency coordination, Sovereign Accelerator formation — so that my contribution to securing governmental anchor participation earns Quantum Privacy Rewards, with the sovereign entity's participation triggering Cascade Premium allocation across all downstream government-sector and regulated-industry adoption.

8.6 The Stealth Intrapreneur (Developer / Engineer)

As a Senior Engineer at a Tier-1 Bank working on internal QPN pilots, I want to commit code — Privacy Pipe configurations, Privacy Agent integrations, Trust Block generation logic — using my corporate laptop and IDE, with each commit's hash signed by my QPC key, so that I accrue verifiable attribution for my architectural contributions without exposing any source code outside my employer's network, earning Operational Activation Quantum Privacy Rewards as the pilot generates real Exchange Token settlement.

8.7 The AI Orchestrator (AI Researcher / Developer)

As an AI Researcher using tools like Claude Code or Copilot, I want to generate a Proof of Orchestration that cryptographically verifies I guided the AI to a specific breakthrough — a novel Privacy Algorithm, a Trust Taxonomy mapping, or a cross-domain interoperability solution — so that the intellectual merit is attributed to me as the orchestrator through my QPC, earning Innovation Premium weighting on Quantum Privacy Rewards.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

8.8 The Trust Architect (Compliance / Governance Specialist)

As a compliance architect with deep expertise in healthcare regulatory frameworks, I want to author Trust Criteria sets that encode domain-specific regulatory requirements into machine-verifiable rules within the Unified Trust Model and earn Proof-of-Trust Accreditation, so that my Trust Criteria become the governance DNA referenced by every Trust Block in healthcare Exchange Networks — earning Exchange Tokens proportional to downstream utilization while ensuring end-to-end regulatory compliance is machine-verifiable rather than assumed.

8.9 The Jurisdictional Bridge-Builder (Regulatory Technology / Legal Specialist)

As a regulatory technology specialist with multi-jurisdictional expertise, I want to create machine-interpretable semantic mappings between Trust Criteria authored for different jurisdictions — HIPAA to GDPR, FDA to EMA, US state privacy laws to each other — so that my cross-jurisdictional mappings unlock previously siloed markets and earn Exchange Tokens on every cross-jurisdictional settlement that relies on my mappings for interoperability.

8.10 The Sovereign Gig-Worker (Freelancer / Independent Contributor)

As a Freelance Developer who has contributed across multiple Accelerators, I want to export my entire history of contributions — code hashes, orchestration proofs, cross-verification records, and classification metadata — into a portable .qpn archive signed by my QPC key, so that I can instantly prove my verified track record to any new employer or Accelerator without relying on any single platform, and my contribution records survive job changes, device loss, and organizational restructuring.

9. Catalyst Networks and Collaborative Contributions

The Quantum Privacy Catalyst Network is the interconnected network of Personal, Enterprise, and Accelerator Catalyst Networks through which contributions are discovered, verified, coordinated, and settled. Its value depends on contributors being able to discover each other, verify each other's claims, coordinate on shared objectives, and resolve disputes — all while maintaining the privacy guarantees that make dual-use contribution possible. This section describes the Catalyst Network hierarchy, Quantum Reputation, and the visibility, coordination, graph assembly, and reward-sharing mechanisms that enable decentralized collaboration at ecosystem scale.

Personal Catalyst Networks

Each individual’s Personal Catalyst Network is the subgraph of the global contribution graph anchored by their QPCs. It encompasses their contributions across all programs and Accelerators, the contribution chains they participate in (including chains initiated by others that pass through their contributions), the people and organizations they’ve connected, the Resources they’ve enabled or provided, the Exchange Networks and Resource Pools they’ve helped form, and the downstream settlement activity their graph has generated. The Personal Catalyst Network grows with every contribution, every chain connection, every objective achieved — and it is permanently associated with the individual’s QPC, portable across employers, Accelerators, and jurisdictions.

A contributor’s Personal Catalyst Network is visible through their QPN Catalyst profile — the contribution portfolio, chain visualizations, reputation signals, and objective alignment that together form a verified professional identity artifact. “Grow your Catalyst Network” is the fundamental call to action: every introduction, every meeting, every partnership advanced, every resource contributed extends the graph, deepens chain connections, and increases Quantum Reputation.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Enterprise Catalyst Networks

An enterprise's Catalyst Network is the aggregate graph of contributions made by and through that enterprise — its employees' work-related Personal Catalyst Network contributions (to the extent visibility settings permit aggregation and the contributions relate to the enterprise's programs, Accelerators, or Exchange Networks), its direct institutional contributions (Resources provided, infrastructure enabled, Exchange Networks anchored), its customers' enrollments and activity, and the settlement flows its infrastructure processes. When an enterprise sponsors an Accelerator or activates Institutional Mode, its Enterprise Catalyst Network densifies dramatically as retrospective processing surfaces historical contributions from institutional data stores.

Enterprise Catalyst Networks are competitive assets. An enterprise with a dense, well-connected Catalyst Network — spanning multiple Exchange Networks, anchoring deep Resource Pools, and demonstrating high Quantum Reputation across domains — attracts more routing, more reuse, and higher MUM than an enterprise with a sparse or isolated graph. This creates direct economic incentive for enterprises to encourage and support their employees' Personal Catalyst Network growth, because every employee contribution that connects to the enterprise's Exchange Networks increases the enterprise's overall graph density and MUM.

Accelerator Catalyst Networks

Each Accelerator Catalyst Network encompasses the contribution graphs of all participants within that Accelerator's programs and objectives — the combined Personal and Enterprise Catalyst Networks of every contributor, plus the institutional contributions specific to that Accelerator (governance frameworks, trust taxonomies, compliance architectures, Resource Pool formation). Accelerator Catalyst Networks compete for participants based on the quality of their programs, the density of their contribution graphs, the MUM of their Exchange Networks, and the Quantum Reputation of their anchor participants.

Quantum Reputation

Quantum Reputation is the derived property of a participant's Catalyst Network and Privacy Networks — a multidimensional, contextual, earned assessment of what they have built, who they are, how they conduct themselves, and how much value they have generated.

It accrues along three complementary dimensions:

- **Contribution reputation** reflects what the participant has done. It is computed from the Catalyst Network's structural properties:
  - **Outcome confidence:** How strongly contributions connect to verified outcomes (the 5-tier confidence model: highest/high/medium-high/medium/lower).
  - **Chain participation:** Depth and breadth of contribution chains — contributions that initiated chains leading to major outcomes earn higher reputation than isolated contributions.
  - **Objective advancement:** Contributions linked to completed program objectives, weighted by objective priority (Essential/High Value/Stretch).
  - **Evidence quality:** Strength of evidence attached to contributions (strong/medium/weak), reflecting the verifiability of the contribution record.
  - **Cross-domain breadth:** Contributions spanning multiple programs, Accelerators, and domains demonstrate versatility and network-building range.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

  - **Downstream settlement value:** The total Exchange Token settlement generated by activity that traces back through the participant's Catalyst Network.

- **Identity reputation** reflects who the participant is and the trustworthiness of their attestations. It accrues from verified identity credentials, professional qualifications, organizational affiliations, and relationship confirmations — each recorded as Trust Credentials within the participant's QPC. A longer contribution history, more activity across programs and domains, more verified relationships, and more third-party validations and endorsements collectively establish that a participant is real, active, and accountable — making it progressively harder to fabricate a credible Catalyst Network as part of a fraud scheme.
- **Behavioral reputation** reflects how the participant conducts themselves — the ethical quality of their interactions, the fairness of their commercial terms, the accuracy of their endorsements and Referrals, the impact of their Resources on counterparties and downstream participants, and their track record of honesty, cooperation, and responsible stewardship across the ecosystem. Behavioral reputation is where the Ethics Premium, Safety Premium, and the endorsement accountability mechanism directly feed in: a participant could have strong contribution reputation and strong identity reputation but weak behavioral reputation if their commercial terms are extractive, their endorsements are unreliable, or their Resources underperform.

All three dimensions are contextual (a participant may have high reputation in healthcare governance and lower reputation in fintech infrastructure), portable (they travel with the QPC and are verifiable through the Contribution Ledger), and durable (unlike platform-dependent ratings that disappear when you leave a platform, Quantum Reputation is anchored in cryptographically verified contribution records that persist independently of any employer, platform, or intermediary).

Referrals and Endorsements

Quantum Reputation is independently valuable because it makes participants more effective at network formation. A participant with a large, well-evidenced Catalyst Network can serve as a credible channel for making introductions, proposing terms of exchange, contributing resources to Exchange Networks and Resource Pools, and connecting participants and proposals to the right counterparties. Two distinct mechanisms enable this:

- **Referrals** provide access and visibility without staking reputation. A participant can use their Catalyst Network to refer another participant, Resource, or proposal to a specific counterparty — leveraging their connectivity and relationships to facilitate access that the referred party could not achieve independently. Referrals are valuable even when the referring participant lacks the domain expertise or direct knowledge to evaluate the quality of what they are referring, because the value lies in the connection itself: routing the right proposal to the right decision-maker at the right time. Referrals are recorded as contributions in the referring participant’s Catalyst Network, extending their graph and earning attribution for the downstream activity the referral generates — without putting their Quantum Reputation at risk if the referred party or proposal underperforms.
- **Endorsements** provide access, visibility, and a reputation-backed attestation of quality. When a participant endorses another participant, Resource, or proposal, they are staking their Quantum Reputation on the endorsement — signaling to the counterparty that they have evaluated the endorsement and believe it to be credible, capable, or valuable. Endorsements carry more weight than referrals because they carry the endorser’s reputation, making counterparties more likely to act. But they also carry accountability: if

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

the endorsed participant, Resource, or proposal turns out to be fraudulent, materially misstated, or significantly underperforming, the endorser's Quantum Reputation is negatively affected — reflecting the failed attestation in their contribution record.

The distinction between referrals and endorsements allows participants to leverage their Catalyst Networks at every level of confidence. A participant with deep expertise in healthcare governance can endorse a specific trust framework proposal with full backing of their reputation. The same participant can refer a fintech startup to an Exchange Network they're connected to — providing valuable access without claiming expertise they don't have. Both activities are contributions that extend the participant's Catalyst Network, but they entail different levels of reputation commitment and influence on the counterparty's decision.

Reputation as accountability. The endorsement mechanism creates a structural incentive for honesty and diligence: participants who make careful, well-founded endorsements build reputation over time, while participants who endorse carelessly or dishonestly erode it. The accountability mechanism is self-enforcing — it operates through the contribution graph and reputation engine without requiring centralized adjudication, because the outcomes of endorsed activity are observable through the same settlement and chain-tracking infrastructure that records all other contributions. The referral mechanism ensures that accountability does not suppress connectivity — participants can always facilitate access through referrals without risking their reputation, thereby keeping the network open and well-connected even as the endorsement layer maintains quality and trust.

This dynamic embodies a mode of preferential attachment: high-reputation participants attract more referral requests, more endorsement opportunities, and more influence over how Exchange Networks and Resource Pools form — not because the system assigns them privileged access, but because other participants rationally seek out credible, well-connected, and accountable counterparties. The result is a merit-based flow of capital and attention — a structural property of the QPN in which economic advantage accrues to demonstrated contribution, verified identity, and trustworthy behavior rather than to institutional position or capital accumulation. MUM itself is an emergent property of the Exchange Network's underlying Resources and relationships; Quantum Reputation influences MUM indirectly by making participants more effective at forming, growing, and interconnecting the networks from which MUM emerges.

Quantum Reputation's Relationship to Proof of Trust: Quantum Reputation is the human-visible expression of what Proof of Trust produces at the infrastructure level. Where Proof of Trust evaluates Trust Criteria compliance and produces Grant or Deny authorization decisions at the machine level, Quantum Reputation aggregates the outcomes of those trust evaluations into a participant-level assessment that is meaningful to humans, enterprises, and governance frameworks. Reputation is a derived property of trust verification, not a separate concept.

9.1 Contribution Visibility Model

Every contribution record has a contributor-controlled visibility tier that determines who can see it, plus granular field-level disclosure controls that determine what they see within that tier.

Tier	Visible To	What Is Visible	When to Use
PRIVATE	**Contributor only**	Encrypted with contributor's QPC key. No manager,	Sensitive or employment-

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

		participant, or counterparty access.	constrained contributions.
MANAGER	**Contributor + Managers**	Classification, impact, opaque entity references, cascade indicators visible. No raw content or PII.	Standard operating visibility. Enables oversight and QP Reward allocation.
PARTICIPANT	**Contributor + Managers + Participants**	Classification, display name/pseudonym, target organization (at authorized level), cascade connection points.	Open collaboration. Peer discovery and graph extension.
VERIFIED_PUBLIC	**All above + Verification invitees**	Includes explicit invitation for counterparties to confirm and join the graph.	Outreach where counterparty confirmation strengthens attribution.

Granular Disclosure Controls:
Within each visibility tier, contributors control field-level disclosure across five dimensions: organization identity (opaque hash to full entity detail); contact identity (opaque to full name, requiring confirmation); classification (visible above PRIVATE; confidence score visible to managers only); temporal (exact to “recent” only); and contributor identity (full name, pseudonym, role descriptor, or anonymous).

9.2 Delegated Attribution: Recording Contributions on Behalf of Another Contributor

Delegated Attribution is the ability to create a contribution record attributed to a named contributor other than the person operating the Capture Tool. It is available across all Capture Tools — a Manager witnessing an introduction at an in-person event can record it via VoiceVector; a team recorder logging a signed agreement can record it via DocVector or the Manual input mode; a MessageVector proxy address can generate a Delegated Attribution record when a contact's inbound message should be credited to the contributor who established the relationship rather than the proxy owner. The attribution logic, governance constraints, and confirmation workflow are identical regardless of which Capture Tool generated the record.

Use cases:

- **Manager-initiated capture:** An Accelerator Manager observing ecosystem activity can record contribution events they witness on behalf of contributors who are not yet using the app — for example, logging that a participant made a key introduction at an in-person event or verbally committed to a partnership.
- **Team-level recording:** A designated recorder on a working team can log contributions for all team members from a single session, attributing each record to the correct QPC without requiring every team member to be present.
- **Administrative back-fill:** During Phase 0, Managers can ingest historical contribution data by recording on behalf of early contributors who participated before any Capture Tool was available.
- **Relationship handoff:** When a contributor introduces a contact to another contributor and the subsequent engagement generates contribution-worthy activity, the introducing

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

contributor can record the downstream activity as Delegated Attribution with a Referral linkage to their original Introduction record — maintaining the full cascade chain without requiring the downstream contributor to self-report.

Governance constraints:

Delegated Attribution records are created with a PENDING_CONTRIBUTOR_CONFIRMATION status and are not eligible for Quantum Privacy Rewards until confirmed. The Attribution Recipient — the contributor to whom the record is attributed — receives a notification via their preferred channel (app notification, email, or encrypted messaging) and must explicitly confirm the record before it becomes ACTIVE. Unconfirmed Delegated Attribution records expire after 30 days and are archived rather than deleted, preserving the audit trail while removing them from active reward consideration.

The Delegating Recorder's identity is logged as a distinct Recorder field in the Attribution Record, separate from the Contributor field. This establishes accountability for the submission and enables anomaly detection: patterns such as a single recorder submitting large volumes of Delegated Attribution records for others, or a recorder and recipient who have no prior interaction history, are flagged for Accelerator Manager review before the records are activated. The compliance screening layer (PPCS/FCFPS) applies to Delegated Attribution records at activation, not at submission, ensuring that confirmation by the Attribution Recipient does not bypass eligibility verification.

9.2 Connection Strength: The Contributor-Facing Confidence Signal

The Attribution Confidence Hierarchy (defined in B.8) is an internal graph assembly metric. Its contributor-facing expression is the Connection Strength indicator, displayed in the contributor's Profile and on individual contribution records. Connection Strength translates the technical confidence hierarchy into an actionable signal that contributors can improve through their own behavior. Connection Strength levels correspond directly to the Attribution Confidence Hierarchy tiers:

Connection Strength Label	Underlying Confidence Tier	What the Contributor Can Do To Improve It
Verified (green badge)	Bilateral Cross-Verification (1.0)	Already at maximum — no action needed.
Strong	Enterprise Corroboration (0.85) or Multi-Participant Triangulation (0.80)	Request cross-verification from counterparties; attach additional evidence.
Building	Temporal + Organizational Overlap (0.65)	Link the contribution to a program objective; attach supporting evidence.
Linked	Classification + Context Inference (0.50)	Provide richer narration; attach evidence; request counterparty confirmation.
Status-Only	Single-Source Claim (0.30)	Attach evidence; request cross-verification; add related contributions to build a chain.

The Profile page displays an aggregate Connection Strength bar showing the distribution of the contributor's records across tiers (e.g., "2 Verified · 1 Strong · 8 more"), with a "Show details" link that expands to the full per-contribution breakdown. This surfaces the cross-verification and evidence-attachment incentives directly in the contributor's experience — making the pathway from a low-confidence to a high-confidence record explicit and actionable.

9.3 My Network: Contributor Activity Analytics

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

The contributor Profile page includes a My Network panel displaying aggregate analytics across the contributor's full contribution history:

Metric	Definition
Organizations	Total distinct organizations referenced across all contribution records.
People Connected	Total distinct contacts referenced across all contribution records, with at least one confirmed identity attribute.
Programs Active	Number of Accelerator Programs the contributor has tagged at least one contribution to.
Contributions Made	Total confirmed contribution records attributed to this contributor (Mine count).
Recorded for Others	Total confirmed contribution records attributed to other contributors by this contributor (For Others count).

Below the summary counts, a contribution type breakdown shows the distribution of the contributor's records by Engagement and Major Milestone type (e.g., Introduction × 2, Meeting × 4, Amplification × 1, Referral × 1, Strategic Partnering MOU Signed × 3). This breakdown enables contributors to assess the shape of their portfolio — and to identify contribution types they have not yet utilized — without requiring them to navigate the full activity log.

9.4 Coordination & Opportunity Marketplace

Contribution Bounties: Accelerator Managers and participants publish structured descriptions of needed contributions, contacts, capabilities, or deliverables with explicit Quantum Privacy Rewards sharing terms. Manager-posted bounties reflect strategic Accelerator priorities; participant-posted bounties enable collaborative fulfillment when a contributor identifies an opportunity they cannot pursue alone.
Bounty Structure: Description, classification category, impact estimate, Accelerator context, reward terms (applicable premiums, cascade sharing, special allocation terms), eligibility requirements, expiration, and visibility level.
Capability Signaling: Participants publish standing descriptions of available expertise derived from their CCP activity summary. Capability signals operate under the same granular disclosure controls — a contributor can advertise “Healthcare executive with C-suite access” without disclosing name, employer, or specific contacts. Identity details exchange only when both parties agree to connect.
Graph Coordination Dashboard:

- **Engagement Map:** Visualization of the contribution graph showing active nodes, cascade chains in progress, and structural gaps.
- **Gap Analysis:** Automated identification of contribution gaps that directly inform bounty creation.
- **Coordination Matching:** Algorithmic suggestions when a participant’s capability matches a posted bounty or another participant’s active engagement.
- **Cascade Progress Tracking:** Real-time visualization of how cascade chains are growing downstream.

9.5 Nearby Opportunities: The Contributor-Facing Objective Feed

The Nearby Opportunities panel on the contributor dashboard surfaces active program objectives that are relevant to the contributor's existing activity — not all objectives across all programs, but specifically those where the contributor's contribution history creates a meaningful pathway to

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

completion. The panel is generated by the Coordination & Opportunity Marketplace engine using three signals:

- **Contribution proximity:** Objectives that reference organizations, contacts, or contribution categories that appear in the contributor's existing records. A contributor who has logged meetings with Pacific Health Systems will see objectives related to payer partnerships before they see objectives related to provider networks.
- **Progress gap:** Objectives that are partially complete — where some contributions have already been made toward the goal but additional contributions are still needed. These are labeled with their progress (e.g., "2/2 — Contributing" for complete, "0/1 — 1 more needed" for in-progress) so contributors can see exactly how their next action moves the needle.
- **Status labeling:** Each opportunity is labeled with the contributor's current relationship to it: Contributing (the contributor's existing records already count toward this objective), Nearby (the contributor is one or two steps away from contributing based on their contact or organization graph), or Available (the objective is open but the contributor has no prior connection).

This is distinct from the Manager-set Bounty system. Bounties are explicit financial incentives created by Managers for specific high-priority tasks. Nearby Opportunities are automatically generated by the system based on graph proximity and objective progress — they require no Manager action and surface value without requiring contributors to browse a bounty marketplace. The two systems are complementary: a Bounty on an objective makes it appear higher in the Nearby Opportunities feed for eligible contributors.

9.6 The Graph Assembly Problem

The QPN/PNX ecosystem is designed for highly decentralized development where contributions arise independently across hundreds of participants, organizations, and Accelerators — often without contributors being aware of each other. The Global Graph Assembly Engine systematically combines fragmentary contribution graphs into a unified global graph, enabling accurate Quantum Privacy Rewards allocation for cascading adoption. Four structural challenges define the assembly problem:

Fragmented chains: A cascade from introduction to deployment may involve five to ten participants, each recording their segment independently. No individual .qpn archive contains the full chain.

Parallel paths: Multiple participants may engage the same organization through different contacts, business units, or value propositions. The graph must represent and attribute both.

Invisible intermediaries: Many contributions occur through intermediaries who may not yet be Catalyst participants — executive assistants, internal champions, board members. Their role may only become visible when they later join or when other records provide corroboration.

Cross-Accelerator linkages: A compliance framework from one Accelerator may be reused by another. These linkages are invisible within any single Accelerator’s graph.

The Graph Assembly Engine

Fragment Linking: The engine identifies records from different participants referencing the same organization, time period, Accelerator context, or milestone event, and evaluates whether they form a causal chain. Linking operates on classification metadata, temporal proximity, and organizational overlap — not on raw content.

Retrospective Chain Reconstruction: As new records accumulate, the engine periodically re-evaluates existing fragments. A contribution that was isolated when first recorded may become linkable months later. This is particularly powerful for multi-step cascades where originators and decision-makers were unaware of intermediate participants.

Enterprise Graph Densification: When enterprises authorize internal systems (email, Slack, DocuSign, Jira, Salesforce) for dual-use Catalyst integration, graph density increases by orders of magnitude. Every internal interaction becomes a potential corroborating node. Because the

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

only output is graph assembly and QP Reward allocation — not content exposure — enterprises face no data leakage risk.

Cross-Accelerator Graph Synthesis: The engine operates across Accelerator boundaries (subject to governance policies) to identify and attribute cross-Accelerator linkages, governed by the EP3 Foundation's Proof-of-Trust Accelerator for global graph integrity.

Attribution Confidence Hierarchy

Evidence Type	Confidence	Description
Bilateral Cross-Verification	**Highest**	Both parties confirm through the cross-verification protocol.
Enterprise System Corroboration	**Very High**	Internal records from dual-use integration independently corroborate the chain.
Multi-Participant Triangulation	**High**	Three or more independent participants' records converge on the same event.
Temporal + Organizational Overlap	**Medium**	Same organization, overlapping timeframes, compatible categories.
Classification + Context Inference	**Lower**	AI inference suggests a likely connection. Flagged for review.
Single-Source Claim	**Baseline**	One participant's unverified record. Valid but carries no corroboration weight.

Higher-confidence linkages carry greater weight in reward calculations, creating natural incentives for participants to increase confidence by sharing at higher visibility tiers, inviting cross-verification, and encouraging enterprise integration.

9.7 AI-Assisted Dispute Resolution

Evidence Search: The Resolver searches the global graph for independent records that corroborate or contradict the disputed contribution.

Alternative Path Identification: If the dispute cannot be corroborated, the Resolver identifies alternative contribution pathways that would achieve equivalent ecosystem value — transforming disputes into constructive ecosystem-growth opportunities.

Retroactive Resolution Queue: Unresolvable disputes are queued for periodic re-evaluation as new records accumulate. Sparse-graph disputes may become trivially resolvable with later enterprise integration.

Confidence-Based Auto-Resolution: Sufficient-confidence resolutions are applied automatically. Insufficient-confidence disputes escalate to Accelerator Managers with the AI's full analysis, evidence chain, and suggested resolutions.

9.8 Reward Sharing: Automatic Attribution vs. Negotiated Bounty Terms

Automatic Attribution Through Graph Structure. By default, each contributor's share is determined by the contribution graph — classification, timing, scarcity, and downstream impact — as evaluated by Quantum Rating Schemes and the applicable premium framework (Strategic, Timing, Value, Cascade, Publicity premiums for bootstrapping; Governance Premiums for enduring values; Adaptive Premiums for self-correction). No explicit reward-sharing agreement is needed for standard graph attribution.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Negotiated Reward Sharing for Bounties. Bounty reward terms define how the participants' combined share is divided between them — not the absolute amount, which depends on the graph's total downstream impact. Negotiated terms operate within the QP Rewards framework, ensuring compatibility with the Proportionality Premium.

9.9 The Impact Score

The Impact Score is a composite quality metric, visible to contributors in their Profile, that summarizes the overall strength of their contribution portfolio along four dimensions. It is distinct from XP (which measures activity volume and consistency) and from Quantum Privacy Rewards weight (which measures economic value enabled). The Impact Score measures how well the contributor's contributions are connected to verifiable, real-world outcomes.

Dimension	Definition	Weight in Score
Evidence Attached	Percentage of contribution records that have at least one piece of supporting evidence attached (document hash, email header metadata, meeting confirmation, file upload).	**~30%**
In Outcome Chains	Percentage of contributions that appear in at least one multi-hop cascade chain — i.e., they are linked (via "Related to") to at least one downstream contribution record.	**~25%**
Linked to Objectives	Percentage of contributions that are linked to at least one active program objective by the contributor or by an Accelerator Manager through the Objective Linking interface.	**~25%**
Major-Tier Contributions	Percentage of contributions classified as Major-tier (high-impact contribution types: Strategic MOU Signed, Enterprise Customer Added, Accelerator Participation Confirmed, Financing Term Sheet / Investment, etc.).	**~20%**

The Impact Score is calculated continuously as new contributions are added and new linkages are established. It is not a static snapshot — a contribution recorded months ago that subsequently appears in an outcome chain retroactively improves the contributor's score. This creates a sustained incentive for contributors to maintain their CCP, participate in cross-verification, and stay engaged with program objective tracking.

Accelerator Managers see aggregate Impact Score distributions across all contributors in their program, enabling gap analysis: identifying contributors with high XP but low Impact Scores (high volume, low connectivity — suggesting they may benefit from cross-verification encouragement or objective linking) versus contributors with low XP but high Impact Scores (low volume, high quality — suggesting they are highly selective in what they record).

10. Catalyst Network Security & Privacy Architecture

The Quantum Privacy Catalyst Network operates in an environment where the most valuable contributions come from professionals whose employment agreements, IP obligations, and institutional compliance requirements create real or perceived personal risk if their ecosystem-building activity becomes visible.

The privacy and security guarantees that resolve this — enabling contributors to earn Quantum Privacy Rewards and grow their Catalyst Networks without exposing proprietary content, employer relationships, or personal identity — are not policy commitments or contractual promises. They are engineering properties of the system architecture, enforced

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

cryptographically, and are structurally incapable of being overridden by any administrator, manager, or governance decision. This section describes the foundational mechanisms that collectively ensure cryptographic record integrity, contributor sovereignty, zero-knowledge verification, governed-agent authorization, coercion resistance, and graph-assembly privacy across the Catalyst Network.

10.1 Cryptographic Record Integrity

Contribution records are created as Contribution Verifiable Credentials (fact records) wrapped inside Trust Block Verifiable Credentials (governance envelopes). The inner signature attests to content; the outer signature attests to governance context. This dual-credential structure ensures that a verifier can check both the factual claim and the governance conditions under which it was recorded in a single operation. Privacy operations — visibility changes, disclosure adjustments, Privacy Seal application — are documented in the Trust Block wrapper without modifying the original fact record. Fact issuance, privacy transformation, and governance attestation are cleanly separated, ensuring that the integrity of the contribution record is preserved regardless of how its privacy context evolves.

Every contribution is fingerprinted using SHA-256 from a deterministic JSON serialization of receipt-relevant fields (contributor, contact, organization, contribution type, timestamps, evidence, visibility). Keys are sorted alphabetically; mutable system state (AI-generated titles, internal metadata) is excluded from the hash. Receipt verification compares the stored hash against a recomputation from current data, producing one of three states: verified (hash matches), unverified (no hash provided), or mismatch (data has been modified). This provides tamper detection that any participant can perform independently, without trusting any intermediary.

10.2 Zero-Knowledge Foundation

- **Ingress:** The Catalyst Agent has read access only to the specific process memory or file buffer required to calculate the hash. No raw text, source code, or document content is ever transmitted outside the contributor's device.
- **Semantic Firewall:** For CommVector, the local AI reads private text to determine meaning but outputs only a boolean classification and opaque metadata. For the AI Evaluation Pipeline, the AI evaluates content semantically but does not transmit content, PII, or classification results beyond the local session.
- **Derived Views:** When a record is shared at MANAGER, PARTICIPANT, or VERIFIED_PUBLIC tier, the network generates a derived view containing only authorized fields. The raw record is never shared.
- **Opaque Matching:** Coordination matching and graph assembly operate on classification metadata, capability signals, and graph topology — not on PII. Participants are suggested as collaborators because their contribution categories are complementary, not because their identities match.

10.3 Governed Agent Authorization Boundary

As the Catalyst application evolves through its agentic phases (see Section 7.6), the security architecture ensures that increasing intelligence does not compromise contributor sovereignty. The three-plane architecture enforces a strict authorization boundary: the Data Plane is where intelligence operates (contribution detection, chain analysis, opportunity identification, proposal generation), and the Control Plane is where governance operates (policy evaluation, human approval workflows, authorization decisions). No agent action — regardless of how it was initiated — executes without passing through the Control Plane's

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Authorization Server, which evaluates every proposal against deterministic policies. The Authorization Server is strictly deterministic: given a proposal and a policy set, the answer is always the same.

This boundary is especially significant for Ambient Mode, where the agent monitors authorized sources and proposes contributions without explicit human initiation. Ambient signals at any consequence level above Observation always require explicit human approval, even for low-risk actions — because ambient signals lack human intent, and the confirmation requirement compensates for that absence. The governed agent loop (Sense → Interpret → Propose → Authorize → Execute → Verify → Learn) ensures that intelligence is unbounded while execution is bounded by human approval and QPC governance. Every authorization decision is recorded in the Authorization Ledger — an immutable, governance-grade audit trail that answers "who authorized this and why?" independently of the operational logs used for system calibration.

Action Consequence Classification

Every action the agent or an automation pipeline proposes carries a consequence level that determines what governance applies. Four levels create a graduated governance response calibrated to the severity of each action's side effects:

- **Observation** actions are read-only with no side effects — querying the contribution graph, computing reputation scores, analyzing chain state, searching for matching contributions. No approval is required and no Trust Block VC is issued. The agent reads and analyzes freely.
- **Advisory** actions produce informational output to humans — suggestions, drafted nudge text, briefings, proposed links shown to an admin, opportunity recommendations. No approval is required, but attribution is required (the system records that the agent suggested this). No Trust Block VC is issued.
- **Reversible** actions have side effects that can be undone — scheduling a follow-up reminder, drafting an email for admin review, suggesting evidence attachment. Human confirmation is required before execution.
- **Consequential** actions have strong or irreversible side effects — creating or modifying contribution records, linking contributions to objectives, changing visibility, issuing credentials. Human approval plus QPC policy validation are required, and a Trust Block VC is always issued.

The consequence level is defined per skill, not per agent. A chain detection skill produces Observation outputs. A nudge composition skill produces Advisory or Reversible outputs depending on whether it is suggesting text or scheduling a send. A contribution creation skill from ambient input is always Consequential. Embedding the governance requirement in the skill definition ensures that the governance boundary is structural, not discretionary.

The consequence classification interacts with the signal input mode to determine specific governance requirements. Ambient signals at any consequence level above Observation always require explicit human approval — because ambient signals lack human intent, and the confirmation requirement compensates for that absence. Directed signals at Consequential level require human confirmation, and the agent must show the source signal (the email, the Slack message) so the approver can verify interpretation. Active signals at Observation level are fully autonomous. Untrusted signals (forwarded from unknown sources, unverified senders) produce advisory output only — the agent may analyze and summarize for the admin, but must not propose any action with side effects until the signal is verified.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

The Action Proposal Contract

Every proposed action — whether generated by a deterministic automation pipeline or by agent reasoning — must be expressed as a structured Action Proposal before it can be authorized and executed. The Action Proposal carries the proposed action, the skill that generated it, consequence level, input mode and trust level, reasoning type (pipeline-scored candidate versus agent contextual judgment), confidence score, required policy checks, and required approvals. This is the contract between intelligence and governance: the Data Plane produces Action Proposals; the Control Plane authorizes them. The contract makes the governance boundary enforceable, auditable, and independently verifiable.

10.4 Contributor Sovereignty & Consent

- **No Automatic Escalation:** A contribution's visibility tier never increases without explicit contributor action. Cryptographically enforced: PRIVATE records encrypted with contributor's QPC key only; MANAGER adds Accelerator Manager's key; PARTICIPANT adds shared group key.
- **Downgrade at Any Time:** Reducing visibility removes the record from the shared graph. Downstream references retain integrity but lose the upstream linkage.
- **Consent-Gated Identity Exchange:** Identity information is exchanged only at the level both parties authorize. Collaboration terms can be negotiated before either party discloses name, employer, or contact details. Privacy-preserving identity resolution and attribute verification — performed within Quantum Privacy Domains through the EasyAccess Authorization Network — operates independently of contributor-to-contributor identity exchange, enabling accurate cross-organizational record linking and Quantum Privacy Rewards allocation without revealing information to any person, organization, or system.

10.5 Deferred Activation Mechanics

All Contribution Records default to DORMANT. No economic value is transferred, promised, or realized at the time of contribution. Records remain dormant until screened by a Proof-of-Trust Accredited Privacy-Preserving Compliance Service (PPCS) and Financial Crime and Fraud Prevention Service (FCFPS), at which point eligible records are activated for Quantum Privacy Rewards allocation and Exchange Token settlement.

Because the only required outputs of the activation process are Quantum Privacy Rewards and Exchange Tokens delivered to the contributor's QPC — which are not publicly disclosed, do not reveal the details of the underlying contribution to any party, and generate disclosure obligations only to tax authorities upon redemption — there is no inherent reason to destroy contribution records from a privacy, compliance, or reputation standpoint. The privacy architecture ensures that sensitive interactions remain protected regardless of whether the associated rewards are claimed.

Contributors who do not wish to receive economic value from specific contributions may voluntarily redirect the associated Quantum Privacy Rewards to a Public Benefit Trust of their choice. The EP3 Nature & Humanity Trust is the default recipient for voluntarily redirected rewards. This mechanism preserves the contribution's value to the ecosystem — maintaining graph integrity, cascade attribution, and downstream reward accuracy — while ensuring that the contributor bears no economic interest in the outcome.

10.6 Audit Trail Architecture & Permanent Privacy Seal

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

All visibility changes are recorded in the contributor's .qpn archive. The contributor has a complete history of what they shared, with whom, at what disclosure level, and when. This audit trail is PRIVATE by default.

Ledger and Log Separation: Defense Against Attribution Controversy

The Catalyst architecture maintains a strict separation between three immutable ledgers and two operational logs. The Contribution Ledger records facts — what happened, who did it, when, with what evidence. The Authorization Ledger records governance decisions — every grant, deny, approval, and policy applied. The Settlement Ledger records value — retrospective economic valuation that reads only verified Trust Block VCs from the Contribution Ledger. These are permanent records with governance significance.

Distinct from the ledgers, two operational logs serve as calibration data for system improvement. The Data Plane Log records agent proposals, authorization decisions received, eventual outcomes, and all Data Plane LLM observations (extraction attempts, corrections, model input/output pairs). The Control Plane Log records command interpretations, approval workflow framing, and human corrections to command parameters. Both logs are working memory — they answer “how well is the system performing?” and “what should it do differently?” — and are purgeable after learning.

This separation is the single strongest architectural defense against future token attribution controversy. Mixing ledgers and logs creates either logs that cannot be purged (because they contain governance facts) or ledgers that cannot be trusted (because they contain mutable operational data). By maintaining the boundary, the architecture ensures that settlement reads only from verifiable contribution facts in the Contribution Ledger — never from agent decisions, operational state, or mutable calibration data. Catalyst makes no economic claims; PNX governance never dictates what gets recorded. Separate books, separate governance, separate timing.

Permanent Privacy Seal. A contributor may request that specific Contribution Records — or their entire archive — be placed under a Permanent Privacy Seal. Sealed records are cryptographically locked such that they are accessible only to automated, Proof-of-Trust Accredited systems (the PPCS, FCFPS, Global Graph Assembly Engine, and QP Rewards allocation logic) for the sole purposes of compliance verification, graph linking, and rewards calculation. Sealed records cannot be accessed, viewed, decrypted, or disclosed by the contributor, by Accelerator Managers, by Quantum Privacy LLC, or by any other human — including under subpoena, internal investigation, or managerial request.

This mechanism directly addresses coercion risk. A contributor who has sealed their records can truthfully state that they have no ability to access, retrieve, or produce the contents of their Contribution Records, and that no human at any level of the organization possesses such ability. Because the records are provably inaccessible to all human parties, there is no factual basis for compelled disclosure, and any attempt to coerce production would be legally futile. This protection complements the trade-secret and confidentiality protections of the QPCPA (Exhibit B and Section 7) by adding a cryptographic enforcement layer that operates independently of contractual obligations.

Sealed records continue to function within the ecosystem exactly as unsealed records do: they inform graph assembly, contribute to cascade attribution, generate Quantum Privacy Rewards, and flow through the settlement waterfall. The contributor receives the same economic benefit — rewards are delivered to their QPC without revealing the underlying contribution details. The only capability the contributor forfeits is the ability to view, export, or present their own records to a new employer or Accelerator Manager as proof of track record.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

A Permanent Privacy Seal is irreversible. Once applied, it cannot be removed by the contributor, by Managers, or by any governance action. This irreversibility is the source of its protective power: it eliminates the possibility that a future actor — including the contributor under duress — could reverse the seal and expose the records.

10.7 Graph Assembly & Analysis Privacy

The Global Graph Assembly Engine reconstructs cascade sequences, links chain fragments, and densifies contribution graphs across independent, decentralized participants — all without accessing the content of any contribution. Assembly operates exclusively on records at authorized visibility tiers, using classification metadata, opaque entity identifiers, temporal data, Accelerator context, and graph topology — never raw content, decrypted PII, or unauthorized contribution details.

Graph links are structural connections between opaque nodes. Privacy-preserving identity resolution of people, organizations, and systems operates continuously within the assembly process to link contribution records and allocate Quantum Privacy Rewards accurately — matching opaque identifiers across contributions, detecting when different contributors have referenced the same person or organization, and tracing cascade chains to their origins — without revealing identities to any participant, administrator, or external system. The engine can determine that Contributor A's introduction led to Contributor B's partnership agreement, which enabled Contributor C's Exchange Network formation — tracing the full cascade chain and attributing settlement value accordingly — without exposing the names of the people involved, the organizations they represent, or the substance of any conversation or agreement.

Separately, contributors may choose to make their identities visible to other participants — either pseudonymously or with real identities — to facilitate collaborative network development, coordination matching, and cross-verification through the coordination features described in this section. Greater collaboration and visibility increase the likelihood of earning more Quantum Privacy Rewards (because visible contributions generate more chain connections, more cross-verification, and more accurate cascade attribution), but participation in collaborative discovery is entirely optional. A contributor who maintains full privacy still benefits from the system's privacy-preserving identity resolution for graph assembly and reward allocation — they simply forgo the additional attribution density that comes from active collaboration with other participants.

For contributors who require the strongest privacy guarantees but do not want to sacrifice attribution accuracy, graph assembly and chain validation will be performable within Quantum Privacy Domains — the cryptographically bounded computation environments defined by the QPN architecture — once the necessary Privacy Domain infrastructure is fully deployed and Proof of Trust Accredited. Contributors will be able to optionally submit the underlying content of their contributions to a QP Rewards service anchored in a Quantum Privacy Domain via a one-way Privacy Pipe. The submitted content can be validated against the cryptographic hashes already recorded in the Contribution Ledger — confirming authenticity — and then analyzed semantically with complete information to produce more accurate chain linkage, cascade attribution, and settlement allocation than metadata-only assembly can achieve. The Privacy Domain boundary ensures that no content, metadata, or intermediate results are revealed to any person, organization, or external system. The only output that crosses the boundary is the final allocation of Quantum Privacy Rewards, without revealing the underlying basis for those allocations. This gives contributors a choice: maintain metadata-only graph assembly (available immediately, privacy-maximizing, attribution based on classification and topology), or opt into Privacy Domain-anchored semantic analysis (available when infrastructure matures, equally privacy-preserving, with higher probability of earning accurate

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Rewards credit). The Privacy Domain computation model extends naturally to cross-enterprise chain validation, where multiple contributors need their chains linked for accurate attribution but neither party is willing to reveal their contribution details to the other: both contributions enter the Privacy Domain via one-way Privacy Pipes, the chain is validated and attributed within the boundary, and only the resulting reward allocations emerge.

The Quantum Privacy Domain, EasyAccess Authorization Network, and Entanglement mechanisms that enable privacy-preserving Rewards analysis and allocation are the same infrastructure that enables Quantum Privacy Tokens, Entangled Tokens, and the jurisdictional optionality described in Section 6.7. This is not a coincidence — it is an architectural consequence. Quantum Privacy Rewards analysis determines what contributions generated what value; token allocation embodies that determination as economic rights. The analysis is upstream of the allocation, and both operate within the same privacy-preserving infrastructure. A contributor's Rewards are computed within a Privacy Domain, allocated as Exchange Tokens through the same Entanglement mechanisms that enable cross-jurisdictional settlement, and delivered to their QPC through the same EasyAccess Authorization boundary that governs all QPN interactions. No additional infrastructure is required for privacy-preserving Rewards — the QPN/PNX token architecture already provides it.

10.8 Relationship to the QPN/PNX Security & Privacy Architecture

The mechanisms described in this section govern the security and privacy properties of the Catalyst Network specifically — contribution capture, visibility, graph assembly, and reward settlement. They operate within and are consistent with the broader Quantum Privacy Network security and privacy architecture, which provides the foundational infrastructure on which Catalyst Network security depends: Quantum Privacy Cells (the cryptographic identity and governance containers), Proof of Trust (the trust verification and authorization framework), the Unified Trust Model (the governance overlay that enforces Trust Criteria across Exchange Networks and Resource Pools), EasyAccess Authorization (the privacy-preserving authorization mechanism that enables information to be linked and analyzed without revealing personally identifiable information), and Privacy Domains (the computational boundaries within which all processing occurs without exposing sensitive data). The full QPN/PNX security and privacy architecture is described in the primary system thesis (*Quantum Privacy Network: Universal Access, Exchange, Ownership, AI & Abundance*) and the patent portfolio, particularly US 12,316,610 B1 and the provisional filings referenced therein.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

APPENDIX A - *Foundational Enabling Services & Catalyst Modules*

A.1 Introduction & Six-Layer Architecture

Appendix A defines the Foundational Enabling Services and Catalyst Modules organized into six architectural layers. Together these components constitute the complete implementation plan for the QPN and PNX — from the contributor attribution system that enables crowdsourced development, through the core runtime systems that operate the network, to the infrastructure bridges that connect the PNX to every major category of enterprise software, cloud platform, identity system, and financial instrument in the global economy.

The components are organized into six layers reflecting their dependency relationships. Lower layers are foundational; upper layers build on the capabilities below them. Within each layer, all components can be developed in parallel.

- **Accelerator Catalyst Layer** (7 components). The contributor attribution, collaboration, and settlement system that must be operational first — because it is the mechanism through which all other components are crowdsourced, attributed, and compensated. Includes contribution capture (CodeVector, DocVector, AgentVector, CommVector, MeetVector, VoiceVector, MessageVector), AI-assisted evaluation, personal archive and context management, and the settlement controller.
- **Core Runtime Layer** (4 components). The systems that operate the QPN/PNX as a production network: QPC lifecycle management at population scale, the EasyAccess enrollment and adoption infrastructure, the Exchange Network and Resource Pool execution engine, and the Quantum Rating System for trust signaling. These can operate with delegated governance (Stage 1) before the Governance Layer is fully deployed.
- **Cryptographic & Identity Layer** (2 components). The post-quantum cryptographic substrate and the privacy-preserving identity resolution infrastructure. These provide the security and identity foundations that all other layers depend on for privacy guarantees and cross-domain participant matching.
- **Resource Publishing Layer** (10 components). Bridges connecting the PNX to the ten major categories of enterprise software where data, content, and computational resources already reside — from data catalogs and cloud storage to CRM systems, model registries, and audience graphs. Each bridge enables existing enterprise resources to become settleable PNX Resources without migration or duplication.
- **Governance & Compliance Layer** (2 components). The Unified Trust Model Runtime that transforms legal, regulatory, and contractual obligations into machine-interpretable, machine-enforceable policy logic — and the Governance Verification Bridge that connects to external GRC platforms and compliance frameworks. This layer is not required for initial operation inside trusted containment (where governance is delegated to the host's existing controls) but becomes essential for multi-host federation.
- **Exchange, Content & Liquidity Layer** (3 components). The personalized exchange engine that adapts real-time bidding and dynamic pricing for PNX settlement, the AI-powered content generation and settlement engine, and the token platform bridge that connects Exchange Token economics to existing financial infrastructure. The Token Platform component is the only component explicitly sequenced (Track B, activated after settlement mechanics are proven).

The fundamental design principle across all components is dual-use deployment: the QPN does not replace existing enterprise infrastructure — it layers consent-governed, privacy-

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

preserving, settlement-generating capabilities on top of it. Every vendor's existing customer deployment becomes a potential PNX node. Every enterprise's existing data governance becomes a potential Trust Criteria implementation. Every platform's existing identity system becomes a potential EasyAccess Engagement Network.

A.2 Component Summary Table

All effort figures are AI-adjusted developer-months — reflecting only the specialized human expertise required after accounting for AI-assisted development (Claude Code, ChatGPT Codex, GitHub Copilot, Gemini Code Assist). The AI% column indicates the estimated proportion of each component's total development work performed or substantially accelerated by AI tools, already factored into the effort figures shown.

The estimated human labor cost assumes a blended average of $20,000 per developer-month ($240K fully-loaded annualized), reflecting a global contributor pool spanning senior engineers in high-cost markets, mid-level developers, and contributors in lower-cost regions. In the crowdsourced Quantum Privacy Rewards model, these costs are decentralized across Accelerator anchor participants, vendor-donated engineering teams, professional services firms billing to client engagements, and investors funding dedicated Accelerators.

Component	Alpha (dev-mo)	Beta (dev-mo)	GA (dev-mo)	AI%	Value Enabled
ACCELERATOR CATALYST LAYER					
WebVector (Contribution Capture & Admin)	3–5	3–5	6–10	65-75%	Enabling
VoiceVector (Voice & Manual Capture)	1–2	2–4	4–6	65–75%	Enabling
CodeVector (DevOps & Engineering)	0.5–1	1–1.5	2–3	70–80%	Enabling
DocVector (Legal & Partnerships)	1	1–2	2–4	65–75%	Enabling
AgentVector (AI & Research)	1	2–3	3–4	60–75%	Enabling
CommVector (Outreach & Engagement)	1–2	2–4	4–6	55–70%	Enabling
MeetVector (Virtual Meetings & Transcription)	1–2	2–4	4–6	60–70%	Enabling
MessageVector (Messaging & Attribution)	1–2	2–4	4–6	55–65%	Enabling
XP Engine & Contributor Engagement Layer	0.5–1	1–2	2–3	75–85%	Enabling
Personal Archive, Context & Intelligence	1	1–2	3–4	65–80%	Enabling
AI-Assisted Evaluation	0.5–1	1–2	2–4	70–85%	Enabling
Settlement Controller & Graph Assembly	2–3	3–5	6–8	50–65%	Enabling
CORE RUNTIME LAYER					
QPC Lifecycle Automation & Propagation	3–5	6–10	10–15	50–65%	Enabling
EasyAccess Deployment Infrastructure	1–2	3–5	5–7	65–80%	Enabling
Exchange Network & Resource Pool Runtime	5–7	8–12	13–19	45–60%	Enabling
Quantum Rating System Infrastructure	2–4	4–6	7–10	55–70%	Enabling
CRYPTOGRAPHIC & IDENTITY LAYER					
Quantum Privacy & Cryptographic Infrastructure	4–6	7–10	12–18	40–60%	Enabling

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Identity Resolution & Trust Attestation	3–5	6–10	10–15	50–65%	$1T+
RESOURCE PUBLISHING LAYER					
Unity Catalog & Lakehouse Publishing Bridge	1–2	3–5	7–10	50–70%	$20–40T
Cloud Object Storage Settlement Overlay (S3/Azure/GCS)	1	2–3	4–6	60–75%	$500B
Model Registry Descriptor Layer (MLflow, SageMaker, HuggingFace)	1–2	3	5–7	65–80%	$10T
Postgres / MongoDB Native Extension	1	2	4	70%	$500B
API Gateway Settlement Wrapper	0.5–1	1	2–3	75–85%	$2–5T
CRM & Workflow Publishing Witness (Salesforce, HubSpot, ServiceNow)	1–2	3	5–6	60–75%	$100T
CI/CD Build & Artifact Witness (GitHub Actions, Jenkins, GitLab CI)	0.5–1	1	2–3	75–85%	$5T
Enterprise Data Catalog Overlay (Alation, Collibra, Purview)	2–3	4–6	8–10	50–65%	$500B
Tokenization & Entitlement Proof Layer	3–4	6–9	12–18	40–60%	$20T
Audience Graph & Marketplace Generation (LiveRamp, UID2, The Trade Desk)	3–5	6–8	10–14	50–70%	$1T
GOVERNANCE & COMPLIANCE LAYER					
UTM Runtime & Taxonomy Management	3–4	5–8	9–14	55–70%	Enabling
Governance Verification & Compliance Bridge	2–3	4–5	6–8	55–70%	$500B+
EXCHANGE, CONTENT & LIQUIDITY LAYER					
Personalized Exchange & Value-Sharing Engine	3–4	5–8	8–13	50–65%	$100T+
AI-Powered Content & Settlement Engine	1–2	3–4	4–6	70–85%	$10–50T+
Token Platform & Liquidity Bridge (Track B)	3–5	6–9	10–14	45–60%	Enabling
TOTAL HUMAN EFFORT (developer-months)	51–78	97–145	176–254	~65% avg	
TOTAL HUMAN EFFORT (person-years)	4.3–6.5	8.1–12.1	14.7–21.2		
ESTIMATED HUMAN LABOR COST (to GA)			$3.5M–$5M		

***Note**: Accelerator Catalyst Layer components have no independent "Value Enabled" estimates because they are the attribution and settlement infrastructure through which all other components' value flows. Core Runtime and Governance Layer components are marked "Enabling" because their value is measured by the settlement they unlock across all other layers. AI-assistable percentages are conservative estimates based on current tool*

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

capabilities; actual productivity gains over the 18-month development horizon are likely to exceed these estimates.

A.3 The Quantum Privacy Rewards Mechanism: What Motivates Contributors

The aggregate human development effort for all Foundational Enabling Services and Catalyst Modules — estimated at 20–30 person-years to GA — is remarkably modest for a system of this scope and ambition. The Accelerator Catalyst Network and Quantum Privacy Rewards system enable decomposition into thousands of independently completable tasks distributed across a global contributor community, with contributors compensated in Exchange Tokens that appreciate as the network they're building gains settlement volume.

Each component comprises dozens of discrete integration tasks — API connectors, SDK wrappers, schema mappings, test suites, documentation, compliance validation — most of which are well-bounded, independently testable, and highly amenable to AI-assisted development. A single contributor using Claude Code or Copilot can complete a well-scoped adapter task in days or weeks. Multiply this across hundreds or thousands of contributors operating simultaneously across all six layers, and 20–30 person-years of human effort compresses to months of calendar time.

The Quantum Privacy Rewards system aligns with every dimension of what motivates high-quality contributors. Financially, contributors earn Exchange Tokens proportional to the settlement value their contributions enable — tokens that appreciate as the network gains volume, creating equity-like upside for early participants without requiring equity grants or employment relationships. The mechanism operates through the Accelerator Catalyst's attribution pipeline (CodeVector, DocVector, AgentVector, CommVector, MeetVector, VoiceVector, MessageVector) and AI-Assisted Evaluation, which classify, attribute, and track every contribution — whether code, contracts, compliance mappings, Trust Criteria specifications, meeting-captured executive introductions, or business development activity. Early contributors to foundational components (cryptographic infrastructure, identity resolution, the UTM runtime, EasyAccess) earn disproportionate rewards through the Proportionality Premium — reflecting both the higher risk and the higher leverage of foundational work. In terms of recognition and reputation, every contribution is cryptographically attributed, permanently recorded, and linked to the contributor's Quantum Privacy Cell — building a verifiable, portable professional reputation that persists across employers, projects, and career transitions. The Contributor Context Profile ensures that the quality, impact, and specificity of each person's work are visible to future collaborators, employers, and the broader ecosystem. For impact, contributors are not writing code that disappears into a corporate repository, drafting contracts that sit in a law firm's document management system, or crafting business plans, marketing strategies, and executive introductions that evaporate once the engagement ends — they are building infrastructure that reshapes how the global economy handles privacy, data ownership, and value distribution. The attribution system makes the causal chain from individual contribution to economic impact explicit and traceable. And for community and collaboration, the Accelerator Catalyst's coordination tools — bounties, capability signaling, cross-verification, and the Graph Assembly Engine — create a collaborative ecosystem where contributors discover each other, form working relationships, and build on each other's work. The network rewards collaboration structurally: contributors whose work enables others' contributions earn attribution through cascade tracking, making cooperation economically rational rather than merely aspirational.

Quantum Reputation

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Contributors build a Quantum Reputation — a cryptographically verified, lineage-linked, multidimensional assessment of their impact, identity, and trustworthiness across the ecosystem.

Quantum Reputation accrues along three complementary dimensions: **contribution reputation** (what the participant has done — verified contributions, chain participation, objective advancement, cross-domain breadth, and downstream settlement value), **identity reputation** (who the participant is — verified identity credentials, professional qualifications, organizational affiliations, and a history of trustworthy attestations recorded as Trust Credentials), and **behavioral reputation** (how the participant conducts themselves — the ethical quality of their interactions, the fairness of their commercial terms, the accuracy of their endorsements, and their track record of honesty, cooperation, and responsible stewardship).

Quantum Reputation can be personalized to the requirements of specific tasks, domains, or counterparties. A contributor applying for a healthcare data integration bounty can present a Quantum Reputation emphasizing their clinical data experience and compliance credentials; the same contributor engaging a financial services Accelerator can present one emphasizing their settlement infrastructure work — all derived from the same underlying Catalyst Network, all cryptographically verifiable, none requiring disclosure beyond what the contributor chooses. Contributors can make their Quantum Reputation publicly visible to maximize professional recognition, or — like Satoshi Nakamoto's contribution to Bitcoin — remain pseudonymous, allowing the work and its economic rewards to speak for themselves without revealing the contributor's identity.

Quantum Reputation enables two distinct network-formation mechanisms. Referrals provide access and visibility — a participant uses their Catalyst Network to connect another participant, Resource, or proposal to the right counterparty, earning attribution for the downstream activity without staking their reputation on the quality of what they refer. Endorsements provide access, visibility, and a reputation-backed attestation of quality — carrying more weight but also accountability, because failed endorsements negatively affect the endorser's Quantum Reputation. The distinction allows participants to leverage their Catalyst Networks at every level of confidence, ensuring the network remains open and well-connected while the endorsement layer maintains quality and trust.

A.4 An Efficient Market for QPN Bootstrapping and Growth

Together, the mechanisms described above — Quantum Privacy Cells, the Deferred Activation Model, the Accelerator Catalyst, Quantum Rating Schemes, and AI-driven allocation optimization — create a fundamentally more efficient market for bootstrapping and growing the QPN and individual Accelerators than traditional financing and compensation models.

Traditional approaches to incentivizing ecosystem formation — venture capital, equity compensation, finder's fees, consulting agreements, advisory stock — suffer from deep structural limitations. They require upfront negotiation of terms before the value of contributions can be measured; they concentrate ownership based on bargaining leverage, capital position, and institutional access rather than verified impact; they impose disclosure, reporting, and tax obligations at the point of grant rather than at the point of value realization; and they create conflicts of interest that prevent participation by many of the individuals best positioned to drive adoption — including employees of target enterprises, regulated professionals, public officials, and individuals across competing organizations who cannot accept outside compensation.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

The Accelerator Catalyst allocation architecture and the Universal Ownership model systematically eliminate these frictions. Quantum Privacy Cells (QPCs) provide legally ring-fenced, privacy-preserving governance containers in which contributions can be recorded, attributed, and accumulated without creating discoverable assets, reportable interests, or compensation events — until the participant affirmatively activates their QPC and eligibility conditions are satisfied. The Deferred Activation Model ensures that no economic value is transferred, promised, or realized at the time of contribution, preserving compliance across all roles and jurisdictions while allowing the contribution graph to capture and verify ecosystem-building activity from the earliest stages. The Accelerator Catalyst separates contribution capture from economic allocation, establishing attributable, timestamped, cryptographically verifiable records that can later inform Quantum Privacy Rewards distributions once governance and liquidity thresholds are met.

This architecture allows each Accelerator — and the QPN as a whole — to incubate itself from a single Quantum Privacy Cell, much as biological life begins from a single cell that carries the complete genetic blueprint for the organism it will become. The initial Quantum Privacy Cell contains the full architectural specification: the governance framework, the trust model, the attribution logic, the settlement mechanics, and the incentive structure. Within the protected environment of the initial dual-use EP3 Accelerators — analogous to an incubator — this single Cell differentiates, replicates, and specializes. New QPCs form as individuals and enterprises activate participation. Exchange Networks emerge as governed resources connect. Resource Pools aggregate as reusable components are contributed. New Accelerators form as coordination structures mature — each one an independent organism grown from its own founding Cell, carrying the same architectural genome while adapting to its specific domain, jurisdiction, and participant ecosystem.

Quantum Rating Schemes then provide the intelligence layer that makes Quantum Privacy Rewards allocation efficient and outcomes-driven. Rather than relying on fixed-fee schedules, negotiated equity splits, or discretionary bonus pools, the Quantum Privacy Rewards framework draws on multidimensional, privacy-preserving ratings — including Impact Contribution, Network Leverage, Value Amplification, Trust, and Compliance ratings — computed from Proof-of-Trust-verified Trust Blocks and contribution graph lineage. These ratings are continuously recalibrated as real-world outcomes emerge, ensuring that Quantum Privacy Rewards reflect actual value creation rather than upfront estimates, negotiation outcomes, or subjective judgment. AI-augmented rating engines operating within Privacy Domains analyze rating performance, predictive accuracy, and market efficiency to propose optimized allocation formulations, creating a self-improving system in which the quality and fairness of Quantum Privacy Rewards distribution improve with scale.

The result is an allocation market that is simultaneously more inclusive (anyone can participate without upfront negotiation or disclosure), more accurate (Quantum Privacy Rewards are indexed to verified outcomes rather than negotiated in advance), more compliant (deferred activation and eligibility enforcement prevent premature value transfer and allow for preemptive compliance verification), and more efficient (AI-driven optimization eliminates the deadweight losses of bilateral negotiation, information asymmetry, and discretionary allocation). This creates a structural advantage over any competing approach to ecosystem formation — whether venture-funded, corporate-sponsored, or government-directed — because the QPN can mobilize and reward a broader, more diverse, and more capable set of contributors at lower friction and higher accuracy than traditional models permit.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

A.5 Three-Tier Contributor Model

- **Tier 1 — Vendor-Donated Engineering Teams:** Technology vendors assign dedicated engineering teams to build and certify adapters — not only for their own platforms, but for any platform whose well-documented interfaces make rapid connector development feasible. Modern enterprise platforms expose comprehensive APIs, SDKs, and integration frameworks; combined with AI-assisted code generation, a skilled engineering team can build production-quality connectors for competitor platforms as easily as for their own. This transforms adapter development from a defensive exercise into a competitive land-grab: the first team to publish a high-quality connector for any given platform captures the Quantum Privacy Rewards for every downstream settlement event that connector enables — regardless of whether the connector targets their employer's platform or a competitor's. Vendors that limit their engineering contributions to their own ecosystems cede Quantum Privacy Rewards on every other platform's integration to faster-moving competitors.
- **Tier 2 — Dual-Use Contributors:** Enterprise employees, consultants, researchers, and specialists who contribute work products generated within their normal professional roles. Zero incremental effort — the Catalyst Agent witnesses their existing work. Every code commit, signed agreement, AI research session, or executive introduction is captured through the appropriate Capture Tool. The Deferred Activation architecture ensures that the contribution is recorded without requiring any immediate career risk from the contributor.
- **Tier 3 — Independent Catalyst Contributors:** Individual developers, data scientists, compliance specialists, and researchers who contribute independently — building components, writing adapters, performing trust assessments, or creating integration documentation. These contributors operate under the standard Quantum Privacy Rewards model, earning Exchange Tokens proportional to the settlement value their contributions enable.

A.6 Vendor Competition for Foundational Network Position

The Foundational Enabling Services and Catalyst Modules, described in B.11 and B.12, collectively touch the product ecosystems of virtually every major technology vendor in the world. Each component specifies integration with specific vendor platforms — Salesforce, Microsoft, Google, AWS, Oracle, Snowflake, Databricks, Okta, Palantir, Nvidia, and hundreds of others. For each vendor, the question is not whether their platform will be integrated into the QPN, but who builds the first integration, when, who accrues the Quantum Privacy Rewards, and how ownership of the resulting Exchange Networks and Resource Pools is allocated.

Consider the engineering capacity of the vendors whose platforms are specified. Microsoft employs 220,000+ people with $30B+ annual R&D spend. Google, Amazon, and Meta each employ 50,000–200,000+ engineers. Salesforce, Snowflake, Databricks, Oracle, SAP, and Palantir each employ thousands to tens of thousands of developers. The clinical research ecosystem (ICON, Veeva, Medidata, TriNetX) collectively employs tens of thousands. The identity vendors (Experian, TransUnion, LexisNexis, LiveRamp) each have thousands of engineers.

If even 0.1% of these engineering organizations were redirected to component development — a negligible diversion of resources — it would represent hundreds or thousands of developers, far exceeding the estimated 20–30 person-years of AI-assisted human effort required for all Foundational Enabling Services and Catalyst Modules. The entire implementation could be completed in 3–6 months under this model, compared to 18 months with the base crowdsourcing approach.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

The Donation-Competition Model

Vendors assign engineering teams to build adapters not only for their own platforms but for competitor platforms as well — because Quantum Privacy Rewards accrue to the first certified adapter for any given platform, regardless of who builds it. These teams operate under the Accelerator Catalyst framework, contributing code through the standard Quantum Privacy Rewards process, with each connector's contribution graph recording who built it, when, and how much settlement value it enables over time.

Proof of Trust Certification Funding

Vendors fund the assessment and certification of their adapters through the Proof of Trust Accreditation Process. This certification demonstrates to the market that the vendor's platform has been validated as a trusted PNX component — a competitive differentiator in enterprise sales. Alternatively, Trust Authorities and contributors focused on governance and compliance can assess adapter submissions and issue Trust Credentials in exchange for a share of the value derived from the use of the certified resource. This creates a self-funding trust ecosystem: well-certified components are adopted more widely, their Resource Derivatives are more valuable, and the Trust Authorities who certified them earn ongoing settlement proportional to that reuse. Trust and compliance become revenue generators rather than cost burdens — attracting the best auditors, security researchers, and compliance specialists to compete for the opportunity to certify high-value adapters, because their economic return scales with the quality and thoroughness of their assessments.

Foundational Network Position

Vendors whose adapters are certified first and incorporated into the foundational Exchange Networks and Resource Pools gain structural advantage: their platforms become the default infrastructure for early PNX settlement, their adapters accumulate the most transaction history, and their trust profiles become the benchmarks against which later entrants are measured.

A.7 Competitive Frenzy Dynamics: Cascade Trigger Paths

The adoption pattern is not a sequential procurement process requiring specific participants in a specific order. It is a coordination race that can be triggered from any of hundreds — potentially thousands — of independent entry points. The structural conditions: participation cost is trivially low relative to the value at stake; existing infrastructure is immediately usable; upside is asymmetric; lagging is penalized; and public commitment increases perceived inevitability.

Each of the following trigger paths pulls in a different but overlapping set of participants — and every participant pulled in by one path becomes a potential trigger for additional paths:

- A hyperscaler commits and pulls in its enterprise customers, identity partners, and consulting ecosystem.
- A Big 4 firm adopts internally and pulls in its audit clients, their vendors, and their counterparties.
- A single large enterprise connects to the interim PNX and pulls in its entire ecosystem.
- The existing Lokahi Accelerator participants demonstrate settlement value in healthcare.
- A Hedera Council member (Google, IBM, Dell, ServiceNow, FedEx, Nomura, Standard Bank, etc.) deploys an adapter for its own platform and pulls in its customer base.
- A sovereign entity launches a Sovereign Accelerator and pulls in national infrastructure.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- A billionaire founder invests, and their technology company publicly joins as an anchor Accelerator participant — triggering competitive responses from peer firms.
- A professional services firm incorporates QPN adapter development into client engagements across every industry.
- A single consulting firm partner incubates an embryonic Exchange Network with an existing client relationship inside trusted containment, demonstrating settlement value that other partners replicate across their own client portfolios within weeks.
- A financial institution launches a Financial Services Accelerator.
- An identity vendor integrates and pulls in every enterprise using its identity graph.

The critical implication: the probability of cascading adoption depends not on the probability that any one specific participant moves first, but on the probability that any one of hundreds of potential trigger events occurs. Even if each trigger is modest individually, the probability that at least one fires approaches certainty as awareness spreads. The gating constraint is not technology, certification, capital, or any specific partnership — it is awareness and understanding.

A.8 Phase 0: Strategic Rationale in Detail

Phase 0 provides six advantages over waiting for production persistence infrastructure:

1. Immediate capture of high-value early contributions eliminates the reconstruction cost and attribution-confidence degradation that increases with every day of delay.
2. Real contribution data provides dramatically better feedback for developing classification algorithms, entity-resolution matching, graph-assembly heuristics, and CCP generation logic than synthetic test sets.
3. Centralized Manager access during the small-population bootstrap period enables efficient graph assembly, gap analysis, and strategic coordination that would be impractical under fully decentralized zero-knowledge constraints — a deliberate trade-off appropriate for the bootstrap phase.
4. Contributors gain visible confirmation that their records are stored, backed up, and available — the "psychological certainty" that their contributions are claimed and will not be lost.
5. Deployment requires only cloud-service configuration, not software development, enabling launch within days.
6. Because Phase 0 uses the canonical schema and is designed to become a Persistence Adapter (the ManagerHostedAdapter), the transition to production infrastructure is additive rather than disruptive — nothing is thrown away; everything migrates forward through the standard Persistence Router replay mechanism.

Contribution Ingestion Pathways (Phase 0)

Records enter the Phase 0 layer through three pathways:

- **AI-assisted session export (immediate):** Contributors using AI assistants with the EP3 Contribution Context loaded generate classified, entity-enriched Attribution Records conforming to the canonical schema, which they submit through a simple web interface or secure file upload.
- **Manual submission with supporting evidence (immediate):** Contributors submit records through a structured web form based on the QPCPA Exhibit A, with supporting

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

evidence (hashed documents, email header metadata, meeting confirmations) attached and reviewed by Accelerator Managers prior to acceptance.

- **Catalyst Agent upload (Phase 1 bridge):** When the Catalyst Agent becomes operational, it uploads records directly through a secure API that will later be wrapped by the ManagerHostedAdapter.

A.9 Attribution Durability: Protocol-Enforced, Not Host-Dependent

A concern that might arise is whether early contributors' claims to Quantum Privacy Rewards are secure when operating inside a host environment like Milliman's. This concern conflates contractual trust with protocol enforcement. The Accelerator Catalyst architecture specifies attribution durability as a technical property, not a relational one:

- **Deterministic contribution hashing:** Every contribution — whether code, adapter, test suite, compliance mapping, Trust Criteria specification, introduction, ecosystem activation, distribution enablement, regulatory engagement, or any other value-creating activity — is cryptographically hashed at the time of submission, creating an immutable record of what was contributed, by whom, and when.
- **Time-stamped allocation recording:** QP Reward allocation claims are recorded with verifiable timestamps — anchored on Hedera Consensus Service where available, or within the host's governed audit infrastructure during Stage 1 — creating a tamper-evident ledger of proportional claims. Contributors may retain personal copies of their contribution records and timestamp proofs, ensuring that no single entity controls the evidentiary basis for their allocation claims.
- **Versioned allocation logic:** The rules governing how settlement revenue is apportioned to contributions are versioned and governance-constrained. Updates require transparent process and cannot retroactively alter existing claims.
- **Portability:** Attribution records are portable across hosts. A contributor's claims are valid regardless of which environment hosts the component their contribution enabled.
- **Non-retroactive dilution:** The Proportionality Premium mechanism ensures that early contributors' claims are not diluted by subsequent contributions beyond the governance-constrained rules published at the time of contribution.

Milliman may provide additional contractual assurances during the interim period, but the economic durability of contributor claims does not depend on Milliman's discretion. It depends on the Catalyst protocol.

A.10 Data Rights & Consent: Strategically Amendable, Not Structurally Blocking

Within Milliman and Big 4 environments, the data access required for initial PNX operation already exists under primary-use rights:

- **Milliman:** Existing data-sharing agreements across thousands of enterprise sources authorize data linkage, cross-source analysis, AI model training, and derived insight generation as primary actuarial use. No separate consent is required for these activities.
- **Big 4 professional services firms:** Standard engagement terms authorize client data use for service delivery, including training AI models to automate audit, accounting, tax, and consulting functions. Using client data to improve the firm's services to those clients constitutes primary use and does not require separate client consent.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Separate consent becomes necessary only when data is remonetized for purposes outside existing commercial terms. But even this constraint is strategically amendable rather than structurally blocking:

- **Client agreements are routinely amended** as business needs evolve. An amendment permitting PNX participation — especially when it confers competitive advantage, generates revenue share for the client, and strengthens the client's privacy and compliance posture — is commercially normal.
- **Personal Privacy Networks and EasyAccess provide a consumer consent layer** that transforms data governance from a defensive constraint into an economic enabler. Once individuals are enrolled in PPNs, their consent authorizes privacy-preserving reuse generating settlement value for every participant including the enterprise that contributed the data. Moreover, PPN enrollment enables the network to automatically enforce individuals' existing legal, regulatory, and contractual rights to their own data, accounts, and other resources — rights that exist today but are rarely exercised due to friction, complexity, and lack of infrastructure. This creates a powerful incentive for enterprises to contribute resources proactively and participate in the value generated: if they do not, individuals can independently assert their rights and authorize access to the same data through their PPNs, eliminating any upside the enterprise might have captured by making resources available on favorable terms. The choice for enterprises is not whether their data participates in the PNX, but whether they participate in the economics of that participation.

The result: initial PNX operation requires no new consent mechanisms at all. Expansion to remonetization use cases requires commercially routine amendments that participants have economic incentive to execute. The consent layer transforms from friction to fuel.

A.11 Milliman's Incentive Equilibrium: Why the First Hub Wins

Milliman's position as the first accredited PNX hub is best understood not as a trust assumption but as an incentive equilibrium in which participation is dominant and defection is irrational.

- **Existing governance posture:** Milliman's global governance, audit, and compliance controls have been extensively certified and are trusted by regulators, enterprise counterparties, and government agencies worldwide. Mapping these controls into the Unified Trust Model is a relatively straightforward compliance exercise — not a ground-up implementation.
- **Routing centrality value:** The first accredited PNX node captures enormous routing centrality. Every cross-domain settlement that requires linking healthcare data to financial data to marketing data flows through the hub that has the most connected sources. Milliman's existing data-sharing relationships with thousands of enterprises across multiple domains give it a structural routing advantage that compounds with every additional connection.
- **Cheating is economically irrational:** The value of being the trusted PNX hub is a perpetual revenue stream from settlement routing. The value of any one-time cheating event is bounded and finite. For a firm of Milliman's scale and reputation — where reputational and regulatory consequences of trust violations would be existential — the net present value of continued trustworthy operation vastly exceeds the value of any defection.
- **Delay is riskier than participation:** If Milliman does not move to formal accreditation, another entity will — a Big 4 firm, a hyperscaler, or a sovereign entity. Once another hub

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

achieves accreditation, Milliman's routing centrality advantage erodes. Moving first locks in structural advantage; delay forfeits it.

The competitive extension is immediate: if Milliman becomes the first accredited hub, every Big 4 professional services firm faces competitive pressure to replicate. PwC, Deloitte, EY, KPMG, and Accenture each maintain global data management infrastructure, extensive client data access under primary-use terms, and compliance assessment capabilities to self-accredit. Each audits a different but overlapping slice of the Global 1000. Any one of these firms can execute the Milliman model at dramatically larger scale through a four-step pathway:

- **Step 1 — Joint Client Bridge:** Connect the firm's global data infrastructure to Milliman's interim PNX through any joint client — and there are hundreds spanning every industry.
- **Step 2 — Internal Adoption:** The firm deploys the Privacy Network internally to manage client data and enable AI automation of its services — a self-funding path to global PNX scale.
- **Step 3 — Self-Accreditation:** The firm assesses and Proof of Trust-accredits its own global network to become an independent PNX platform.
- **Step 4 — Global Client Cascade:** Internal adoption by any single Big 4 firm is sufficient to catalyze global enterprise adoption. PN-enabled services deployed internally become PN-enabled services offered to the market.

If any one of the Big 4 firms or Accenture were to combine their IT infrastructures with Milliman's, the combined coverage encompasses virtually every major enterprise in the world. In addition to Milliman and the Big 4, any organization with a trusted IT environment and mature security and compliance controls can serve a similar hub role — major banks, hyperscalers, sovereign IT agencies — expanding the number of potential containment hosts to hundreds of qualified entities.

A.12 FISMA and FedRAMP as Accelerants

The compliance framework extends naturally to government adoption. Components deployed within Milliman's or a Big 4 firm's trusted environment inherit the host's existing compliance posture. For federal government use cases, components that achieve FISMA Authorization to Operate (ATO) or FedRAMP certification gain access to the $150B+ federal IT market. But the strategic significance of federal certification extends far beyond government procurement. FISMA or FedRAMP certification of the core Quantum Privacy Network and EasyAccess Authorization Network platform capabilities would serve as a powerful, independently verified trust credential that substantially eliminates adoption risk for any organization — government or enterprise — by demonstrating that the platform meets the most rigorous security, privacy, and compliance standards in the world. Simultaneously, federal certification substantially eliminates the ability of enterprises to safely block enforcement of individuals' data rights: once the infrastructure through which individuals assert their legal rights to data, accounts, and resources carries federal-grade security and compliance certification, enterprises can no longer credibly claim that honoring those rights poses security, privacy, or compliance risks. The platform's trust posture becomes, in effect, superior to the enterprise's own — removing the last defensible basis for resistance. Vendors and professional services firms have powerful economic incentive to pursue these certifications — each certification simultaneously opens the federal market, collapses enterprise adoption barriers, strengthens individual rights enforcement, and generates ongoing Quantum Privacy Rewards and PNX settlement revenue.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

A.13 Embryonic Network Incubation: Bottom-Up & Top-Down Cascade Mechanisms

The Accelerator Network has proactively established Enterprise, Portfolio, and Sovereign Accelerators for every organization, institutional investor, and government on the planet, enabling any individual — executive, employee, partner, vendor, or customer — to make contributions and receive Quantum Privacy Rewards for any of them. The question is not whether the infrastructure exists for participation, but whether and when there is formal sponsorship from the enterprise, fund, or government at the executive level. The architecture supports two complementary adoption pathways that operate independently and reinforce each other.

Bottom-Up Incubation: The Embryonic Multi-Sided Network Pattern

Participation is not a corporate procurement decision at first. It is partner-led, practice-led, or program-led within existing engagements, where adapters are client-funded or dual-use as part of ongoing service delivery, and upside accrues to the participating individuals via Quantum Privacy Rewards.

The smallest viable cascade unit requires only three parties: a practice leader or relationship owner (a Big 4 partner, a consulting firm engagement manager, a technology vendor account executive, a government program director), a client or counterparty whose relationship they own, and a trusted host operating a Privacy Domain (Milliman, a Big 4 firm, or any qualified containment environment). Together, these three parties deploy the adapter layer linking identity, data, analytics, governance, and settlement attribution between the partner's and client's existing IT infrastructure and the interim PNX platform. This is not a pilot, proof of concept, or sandbox exercise. It produces a live, functional micro-ecosystem: a working Exchange Network, a Resource Pool, settlement events, contribution graph entries, and Quantum Privacy Reward allocations — all operating under production-grade governance inherited from the host's existing compliance controls.

The power of this pattern lies in what happens after the first instance exists. Once a single partner or employee has incubated an embryonic network with a single client, every other partner or employee inside the same firm can reuse the same adapters, governance mappings, and attribution logic. Every other client executive can join using the same template. The governance artifacts are already mapped. Risk is de-risked by precedent. Attribution logic is proven. Settlement flow is demonstrated. Replication cost collapses from an integration project to something closer to cloning a network instance — a fundamentally different growth curve.

Top-Down Executive Sponsorship: Faster, More Valuable & Fiduciarily Compelling

While bottom-up incubation can ignite the network without executive approval, top-down executive sponsorship accelerates the cascade dramatically — and the executives who provide it benefit disproportionately more than those who wait for bottom-up validation to make the decision for them. When a CEO, managing partner, agency head, or government minister provides formal enterprise-wide or government-wide sponsorship, the effect is not incremental — it is multiplicative. Instead of one partner incubating one embryonic network with one client, every partner, every practice area, every client relationship, and every employee across the entire organization is enabled to contribute, connect, and earn Quantum Privacy Rewards simultaneously.

Executive sponsorship of QPN/PNX participation does not require incremental investment, new budget allocations, procurement cycles, compliance approvals, technology

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

deployments, or any of the bureaucratic and political barriers that traditionally impede enterprise innovation. It requires only a decision to authorize what the organization's employees, partners, and clients can already do individually — but to do so at enterprise scale, capturing the Quantum Privacy Rewards and settlement economics that would otherwise flow to individuals acting independently or to competing organizations that moved first. The infrastructure already exists. The compliance controls are already in place. The data-sharing agreements are already signed. The only thing missing is the authorization to use them.

The personal economic consequences for the sponsoring executives are proportionally extraordinary. Under the Quantum Privacy Rewards model, the executives whose verifiable contribution graphs include proactive formal enterprise-wide sponsorship — the decision that unlocked thousands of relationship pathways, millions of potential PPN enrollments, and billions in potential settlement volume — earn Quantum Privacy Rewards proportional to the ecosystem value their sponsorship enabled. An executive who sponsors early, before bottom-up incubation forces the decision anyway, captures the full Quantum Privacy Rewards premium for the foundational contribution. An executive who waits for bottom-up validation to eliminate perceived risk earns dramatically less, because the incubators and expanders who demonstrated value in the interim have already captured the foundational contribution rewards. The Proportionality Premium does not reward waiting — it rewards the courage and judgment to act when the structural logic is clear, but the social proof is not yet overwhelming.

The shareholder and public-benefit implications are equally stark, operating through two compounding mechanisms. First, the Leader vs. Laggard dynamics show that an enterprise that delays adoption suffers an 85–86% reduction in the total ecosystem value attributable to its participation — shrinking the entire economic pie available to both the enterprise's direct stakeholders and the individuals and organizations across its ecosystem. Second, of whatever ecosystem value remains, the share that flows to the enterprise itself — and therefore to its shareholders — versus the share distributed across employees, users, vendors, consultants, and other ecosystem participants is determined by who led adoption. When executives provide early, top-down sponsorship, the enterprise captures 25–35% of its total ecosystem value directly for shareholders, with the remainder distributed across the broader ecosystem. When adoption is driven bottom-up by individuals acting independently, the enterprise's direct capture shrinks further because the individuals and organizations that incubated and expanded the network — not the enterprise as an institution — hold the foundational Quantum Privacy Rewards and contribution graphs that command the largest share of settlement economics.

The compounding effect is severe. A laggard enterprise suffers an 85–86% reduction in total ecosystem value, and then captures a smaller proportion of that already-diminished value because grassroots adopters within its ecosystem have already claimed the foundational positioning rewards. The shareholders bear both penalties simultaneously.

For sovereign entities, the same dual mechanism applies with equal force. If governing authorities delay adoption, their citizens, residents, and businesses can still accrue value through individual participation and bottom-up incubation — but the share that flows to the public-benefit trust available to fund citizen services, infrastructure, social programs, and sovereign debt reduction shrinks on both dimensions. The total ecosystem value attributable to the jurisdiction is reduced by the laggard penalty, and the proportion of that reduced value flowing to the sovereign treasury rather than to individual participants is further compressed. Early sovereign sponsorship maximizes both the total pie and the public share of it; delay diminishes both.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Every month of delay is a month in which other enterprises or jurisdictions are establishing the foundational network positions, routing preferences, and trust schema alignments that late movers cannot replicate. Moreover, delay does not merely reduce the total value captured — it redistributes who captures it. In the absence of formal executive sponsorship, employees, vendors, customers, and other ecosystem participants will adopt independently through bottom-up incubation and individual PPNs, earning Quantum Privacy Rewards and capturing settlement economics for themselves. The value that flows through an enterprise's or sovereign entity's ecosystem flows regardless — but without executive sponsorship directing and coordinating that participation, the rewards accrue disproportionately to the individuals and organizations that led adoption rather than to the shareholders, citizens, governmental coffers, or beneficiaries that executives and officials are fiduciarily responsible to serve. Executive delay does not preserve optionality — it transfers wealth from the principals to the agents, from the institution to the individuals, and from the stakeholders as a whole to whichever subset moved first.

This creates a fiduciary and governance imperative that is unusually clear. Executive sponsorship of QPN/PNX participation does not require incremental investment, new budget allocations, procurement cycles, compliance approvals, technology deployments, or any of the bureaucratic and political barriers that traditionally impede enterprise innovation. It requires only a decision to authorize what the organization's employees, partners, and clients can already do individually — but to do so at enterprise scale, capturing the Quantum Privacy Rewards and settlement economics that would otherwise flow to individuals acting independently or to competing organizations that moved first. The infrastructure already exists. The compliance controls are already in place. The data-sharing agreements are already signed. The only thing missing is the authorization to use them.

From a fiduciary perspective, once an executive understands the structural logic — that participation cost is zero, that upside is asymmetric, that delay forfeits durable economic rights to faster-moving competitors, and that employees and clients will participate regardless through individual PPNs and bottom-up incubation — continued delay is not prudent risk management. It is the forfeiture of shareholder or public value without compensating benefit. For corporate directors bound by duties of care and loyalty, and for government officials bound by public trust obligations, the question is not whether the risk of participation justifies waiting, but whether the certainty of forfeited value justifies inaction when participation requires no incremental resources.

A.14 From Execution-Sensitive to Execution-Sequenced: No Remaining Gating Factors

The containment-first architecture removes certification as a timeline constraint. Person-centered aggregation through PPNs and QPCs removes enterprise-to-enterprise interoperability as a federation prerequisite. Contractual interim settlement through Inter-QPC agreements removes on-ledger activation timing as an adoption gate. Universal Compliance removes resource-level accreditation as a scaling bottleneck. Jurisdictional optionality and entangled token embodiment, combined with contractual interim settlement, remove liquidity expansion as a regulatory gating risk.

No structural barriers to adoption remain. What remains is execution sequencing — the ordering and pacing of tasks that are individually well-understood, grounded in existing infrastructure and established operational patterns, and driven by self-organizing incentive alignment rather than centralized coordination. The distinction between a system with gating dependencies and a system with execution sequencing tasks is fundamental: gating

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

dependencies can prevent a system from functioning; execution sequencing affects only the speed and order in which a system that is already functioning expands its scope, efficiency, and scale. The QPN/PNX has no gating dependencies. It has a roadmap.

A.15 Reassessing the Scenario Probability

Under the containment-first architecture, the scenario previously labeled "Aggressive Cascading Adoption" shifts significantly toward base-case probability. The reasons are structural:

- **The primary timeline risk** — certification delay — is eliminated. The containment-first architecture enables all components to be developed, deployed, and generating economic value inside trusted containment environments (Milliman, Big 4 firms, or any qualified host) under existing compliance controls from day one. Proof of Trust accreditation proceeds in parallel with production operation, applied selectively to components that need to externalize — not as a system-wide prerequisite. Lazy certification means the network is never gated by the slowest-certifying component.
- **The primary contributor risk** — attribution insecurity — is bounded by protocol-enforced durability. Deterministic contribution hashing, time-stamped allocation recording with personal contributor copies, versioned allocation logic, and portability across hosts ensure that every contributor's claims are cryptographically verifiable, tamper-evident, and independent of any single host's discretion. The Proportionality Premium protects early contributors from retroactive dilution beyond governance-constrained rules published at the time of contribution.
- **The primary data access risk** — consent and agreement friction — is resolved by existing primary-use rights. Within Milliman and Big 4 environments, the data access required for initial PNX operation already exists under primary-use authorizations — actuarial analysis, audit, advisory, and client service delivery. Separate consent becomes necessary only for remonetization beyond existing commercial terms, and even then is strategically amendable through commercially routine agreement amendments that participants have economic incentive to execute. PPN enrollment transforms consent from friction to fuel by enabling individuals to authorize privacy-preserving reuse that generates settlement value for every participant including the enterprise that contributed the data.
- **The primary scaling risk** — infrastructure capacity — is resolved by elastic cloud deployment. Milliman's core platform operates on Databricks deployed across Azure, AWS, and Google Cloud, with hundreds of millions of dollars in committed cloud infrastructure spend. There is no architectural scalability limit — the only constraint is cloud compute cost, and anyone can cover those costs: hyperscalers as in-kind contributions, AI vendors, enterprise clients as part of engagements, investors, sovereign entities, or settlement revenue generated by the platform itself. The infrastructure inherits production-grade performance, security, and availability from the world's three largest cloud providers without requiring new build-out.
- **The primary adoption risk** — cold start — is resolved by existing institutional relationships and production infrastructure. Milliman's existing data-sharing agreements with thousands of enterprise sources across healthcare, insurance, financial services, and government provide immediate Resource Pool formation. Hedera's Governing Council — including Google, IBM, Dell, ServiceNow, Wipro, Tata Communications, Deutsche Telekom, and others — provides a pre-established network of Global 1000 enterprises with existing technical integration. The Big 4's client relationships collectively span virtually every major enterprise in the world. ICON's 40,000 employees across 50+ countries and relationships

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

with every major pharmaceutical company provide healthcare vertical depth. EP3's 45 Affiliate organizations provide the initial contributor pool. The cold-start problem is architecturally eliminated: the network launches with thousands of pre-existing institutional relationships, not from zero.

- **The primary governance risk** — dynamic policy enforcement — is resolved by delegated governance using configurable enterprise platforms that already manage the relevant data. Unity Catalog provides fine-grained column-level security, row filters, and data lineage tracking. Microsoft Entra ID enforces conditional access policies, role-based access control, and cross-tenant collaboration rules. Snowflake's dynamic data masking and row-level security provide additional governed data access. AWS Lake Formation's tag-based access control governs cloud-native resources. These systems represent billions of dollars in enterprise governance investment, already configured, already audited, and already trusted by regulators — the PNX operates within this governance from day one, with the Unified Trust Model progressively making implicit governance explicit and machine-interpretable as federation requirements emerge.
- **The primary organizational risk** — requiring executive-level sponsorship before participation — is resolved by the embryonic network incubation pattern, where individual partners, practice leaders, and program directors can incubate live micro-ecosystems within existing client relationships, with formal sponsorship emerging as a consequence of demonstrated value rather than as a gating prerequisite. Simultaneously, the top-down pathway is fiduciarily compelling: sponsorship requires no incremental investment, budget, or compliance approvals, and delay forfeits durable economic rights that faster-moving competitors and bottom-up incubators are already capturing.
- **The primary liquidity risk** — that token-based economic rights are meaningless until liquid markets exist — is resolved by three complementary mechanisms: contractual interim settlement through Inter-QPC agreements makes Quantum Privacy Rewards economically binding through conventional commercial mechanisms from day one; jurisdictional optionality ensures that Quantum Privacy Tokens are not bound to any single jurisdiction, with conversion routed to the most favorable regulatory and tax environment at execution time; and entangled token embodiment allows a single QPT to be simultaneously embodied across multiple platforms and jurisdictions, ensuring that no single jurisdiction's regulatory change can impair the holder's economic rights.
- **The primary compliance risk** — that resource-level accreditation cannot scale fast enough to keep pace with adoption — is resolved by Universal Compliance, which routes data through one-way Privacy Algorithms into Quantum Privacy Domains where any computation proceeds under cryptographic guarantees, eliminating the need for resource-level accreditation as a prerequisite for publishing and utilizing resources within the network.
- **The primary interoperability risk** — that cross-host federation requires enterprise-to-enterprise negotiation and protocol standardization before value can flow between hosts — is resolved by person-centered aggregation through PPNs and QPCs, which enables resources to flow through individual-authorized channels without requiring enterprises to negotiate with each other, agree on terms, or even know about each other's participation.

No structural gating factors remain. What remains is execution sequencing — the ordering and pacing of tasks that are individually well-understood, grounded in existing infrastructure, and driven by self-organizing incentive alignment rather than centralized coordination. The scenario that follows should be read not as an aggressive upside case but as a structurally grounded projection.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

A.16 Cascading Adoption Under the Containment-First Architecture

Under the containment-first architecture described above, the scenario previously modeled as "aggressive" shifts toward base-case probability. The following timeline reflects this recalibration: it assumes Protected Proliferation inside Milliman's trusted environment from day one, durable protocol-enforced attribution, existing primary-use data rights, delegated governance through configurable enterprise platforms, layered encryption for source assurance, and the competitive coordination race dynamics that activate once the first major participant publicly commits.

Months 1–3: Ignition & Professional Services Activation

- Core architecture team (20 people) begins work on the Accelerator Catalyst Layer, Core Runtime Layer foundations, and Cryptographic & Identity Layer components, funded through the multiple pathways described above. Development occurs within Milliman's production Databricks/Azure/AWS/GCP environment using Stage 1 delegated governance.
- Hedera activates as a Tier 1 Accelerator: Hedera has already funded EP3, and a preliminary integration has validated the technical viability and architectural fit between Hedera Consensus Service and the QPN's settlement and governance infrastructure. This is not a theoretical partnership — it is a production relationship with demonstrated technical integration.
- Milliman's existing DeltaShare infrastructure is documented and published as the initial Cloud Object Storage reference implementation, immediately available to Catalyst Contributors as a working example of a production Resource Publishing component.
- Anchor enterprise adopter assigns 10–20 engineers to build EHR & Clinical Data adapters against real clinical trial data flows in the Lokahi Healthcare Accelerator.
- Professional services firms engage immediately: PwC, Deloitte, KPMG, Ernst & Young, and Accenture each maintain technology practices employing tens of thousands of engineers and consultants who build enterprise integrations as their primary business. McKinsey and BCG have global client bases and deep c-suite relationships. The QPN represents a new category of billable engagement.
- EP3's 45 Affiliate organizations are activated as the initial QP Catalyst contributor pool. Engineers and data scientists begin dual-use contributions to components relevant to their domains.
- First outreach to hyperscalers and founders: Azure, AWS, and GCP teams — who already support Milliman's multi-cloud infrastructure — are presented with the vendor competition model.

Months 3–6: Investment Cascade & Sovereign Activation

- First major investment: A hyperscaler founder or corporate venture arm invests $250M–$500M in EP3 and launches a dedicated Accelerator. This is rational investment — these founders have individually committed $10B–$100B+ to AI infrastructure with longer payback periods and less certain returns.
- Competitive investment frenzy: The first major investment triggers exactly the competitive dynamic that drives AI infrastructure spending. If one hyperscaler founder invests, the others cannot afford to let a rival establish foundational positioning.
- Billions flow into the ecosystem: Within three months of the first major investment, cumulative investment reaches $1–5B. This capital funds dedicated Accelerators,

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

enterprise onboarding programs, adapter development, and Proof of Trust certification at a velocity that individual Quantum Privacy Rewards alone cannot match.

- Professional services firms formalize: Each launches QPN practice areas. Consulting teams begin incorporating component assessment, incubation, and deployment into client engagements across every industry.
- Hyperscaler engineering at scale: With billions in investment creating competitive pressure, hyperscalers assign 500–1,000+ engineers each across their platform teams. Combined development capacity across hyperscalers, professional services, identity vendors, and Catalyst Contributors exceeds 10,000 developers.
- Sovereign Accelerators launch: The State of Hawaii's Lokahi model is replicated. California, the EU (building on eIDAS 2.0), Singapore, the UAE, and other jurisdictions launch sovereign programs. These do not require head-of-state approval — agency-level champions, public health directors, and innovation officers can independently connect data through existing authorities.
- Contributor count exceeds 5,000–10,000: The development capacity far exceeds what the Foundational Enabling Services and Catalyst Modules require — surplus capacity flows into creating hundreds of additional adapters for regional, legacy, and niche platforms.

Months 6–9: Settlement at Scale

- Multiple Resource Publishing components reach GA simultaneously. With thousands of engineers deployed, the development bottleneck shifts from engineering capacity to Proof of Trust certification and business development.
- Hedera Consensus Service becomes the backbone of settlement audits. Every PNX settlement event is anchored on Hedera's immutable, timestamped consensus layer. Council members begin deploying adapters for their own platforms.
- Healthcare settlement scales through ICON and pharma. Clinical trial data, real-world evidence, and pharmaceutical commercial data flow through EHR adapters.
- Financial services settlement begins. Major financial institutions launch Financial Services Accelerators, building on the financial data and tokenization components.
- Identity Resolution component reaches GA. With every major identity vendor contributing engineering teams, the global privacy graph integrates 20+ vendors within 9 months. Cross-domain match rates reach 85%+ for U.S. adults.
- Monthly settlement volume: $20–$100M. Meaningful revenue across healthcare, financial services, cloud data collaboration, and sovereign data programs.

Months 9–12: Platform Integration & Population-Scale Enrollment

- First major platform EasyAccess integration: A hyperscaler integrates EasyAccess into its consumer platform. Google (3B+ users across Search, Gmail, YouTube, Android), Microsoft (1B+ users across Office 365, LinkedIn, Outlook), or Meta (3.7B monthly active users) batch-enrolls its user base into Personal Privacy Networks.
- Cross-domain settlement explodes: With population-scale enrollment and multiple industry verticals operational, the number of settleable transaction types grows combinatorially. Healthcare data linked to financial data linked to marketing data — all privacy-preserving, all settlement-generating.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- Monthly settlement volume: $100M–$500M. Revenue inflection occurs. The QPN is operating infrastructure generating billions in annualized settlement.

Months 12–18: Dominance

- All Foundational Enabling Services and Catalyst Modules at GA or controlled beta. Full infrastructure stack operational across all vendor platforms, all major cloud environments, all identity vendors, and all industry verticals.
- Cryptographic Infrastructure at GA: Post-quantum cryptographic enforcement, zero-knowledge governance verification, and hardware-rooted trust anchoring deployed across production settlement. Layered encryption becomes standard pattern for all cross-host exchange.
- Governance & Compliance Layer components reach GA: The transition from Stage 1 (delegated governance) to Stage 2 (federated governance) completes for major host pairs. Cross-host settlement operates under machine-interpretable Trust Criteria verified programmatically rather than through manual compliance review.
- Sovereign Accelerators in 15–25 nations. Cross-border settlement between sovereign domains enabled by cryptographic data sovereignty enforcement and cross-domain Trust Criteria mapping.
- Annual PNX settled revenue exceeds $5–$10B and accelerating. The network effect is self-sustaining. Every new participant increases settlement opportunities for every existing participant.
- Vendor revenue-share payments exceed $1B annually. Creating irreversible structural dependency on the PNX.

Months 18–24: Global Standard

- Annual PNX settled revenue exceeds $25–$50B and growing. The PNX has become the global standard for privacy-preserving cross-organizational data collaboration.
- Contributor ecosystem exceeds 50,000 active developers globally. Adapters exist for virtually every enterprise platform, legacy system, and regional technology.
- Stage 3 cryptographic governance begins deployment. Zero-knowledge proofs of Trust Criteria satisfaction, continuous Proof of Trust monitoring, and homomorphic computation on encrypted data extend governance from federated to cryptographic.
- The most capital-efficient investment opportunity ever presented — in any industry, at any scale, in any era. Every prior transformative investment — railroads, electrification, telecommunications, the Internet, mobile computing, cloud infrastructure, AI — required building new physical systems at enormous capital cost. The QPN builds nothing physical. It connects existing systems through software adapters and captures settlement value every time those systems are used for cross-organizational collaboration. The total addressable market is every data interaction that crosses an organizational boundary in the global economy. The direct capital required to ignite it is less than $50M.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

APPENDIX B - *Engineering Specifications*

B.1 Patentable Inventions Summary

A provisional patent application has been filed covering over 400 claims across eighteen invention families based on the architectural content described in this document and related filings. The following inventions represent the primary areas of claim coverage:

- **The Quantum Privacy Sidecar Pattern:** A privacy-preserving witness architecture that observes professional work products without extracting or transmitting content. Novel aspects: the four-component client architecture (Witness Agent, Listener Agent, Local Vault, Verification Bridge), the Sender-Pays / Lazy-Verify computational model, and the deferred-activation DORMANT record state.
- **The Five Signal Input Mode Architecture:** A structurally complete contribution capture taxonomy organized by human intentionality level (Active, Directed, Ambient, Institutional, Evangelized), where the first four modes capture contributions that have occurred and the fifth generates new contributions that would not otherwise exist. Novel aspects: the Evangelized Mode attribution-tracking mechanism (where evangelizers earn settlement-linked rewards proportional to the downstream contribution graphs their distribution generates), the Institutional Mode retrospective graph densification pattern (enterprise-authorized processing of institutional data stores to reconstruct contribution history at scale), and the Ambient Mode governance requirement (ambient signals at any consequence level above Observation always require explicit human approval to compensate for the absence of human intent).
- **The Three-Stage AI Evaluation Pipeline:** An intelligent classification system embedded in contributor AI tools performing (1) Semantic Contribution Classification using causal-enablement logic; (2) Identity Enrichment & Entity Resolution generating multi-attribute identity anchors; (3) Temporal Durability Anchoring linking records to multiple independent identity anchors. Novel aspects: causal-enablement classification model, maximum-attribute-capture-at-minimum-contributor-effort interaction design, cross-session cascade detection architecture.
- **The Global Contribution Graph Assembly Engine:** An AI-powered service that systematically combines fragmentary contribution graphs into a unified global graph. Novel aspects: fragment linking algorithm operating on classification metadata (not raw content), retrospective chain reconstruction as new records accumulate, enterprise graph densification through dual-use integration, cross-Accelerator graph synthesis under EP3 governance, and privacy-preserving identity resolution operating continuously within the assembly process to link records and allocate Quantum Privacy Rewards without revealing identities to any participant, administrator, or external system.
- **The Cross-Verification Protocol:** A bilateral attribution chain mechanism extending CommVector's SENT → VERIFIED_ENGAGEMENT status upgrade. Novel aspects: Prior-Awareness Clarification system with evidence-weighted confidence scoring; asymmetric visibility protecting counterparty confidentiality; Counterparty Context Enrichment with three-tier visibility (AI-Only / Manager-Visible / Manager-Visible with Outreach Authorization); graduated incentive structure rewarding progressively greater disclosure.
- **The Persistence Adapter Architecture:** A substrate-agnostic persistence layer decoupling contribution records from any single storage system. Novel aspects: abstract PersistenceAdapter interface; Persistence Router with configurable resilience strategies (Write-All, Write-N-of-M, Write-Primary-Plus-Backup, Write-Local-Only); replay

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

mechanism enabling retroactive migration to new substrates; Phase 0 ManagerHostedAdapter bootstrap pattern transitioning seamlessly to production architecture without data migration.

- **The Governed Agent Authorization Architecture:** A three-plane architecture (Data Plane, Control Plane, Management Plane) enforcing a strict boundary between intelligence and governance in an agentic contribution capture system. Novel aspects: the deterministic Authorization Server (given a proposal and a policy set, the answer is always the same), the Action Proposal contract carrying confidence, reasoning type, and consequence level as governance-readable metadata, the dual-credential Contribution VC / Trust Block VC nesting model (inner signature attests to content, outer signature attests to governance context, privacy operations documented in the wrapper without modifying the fact record), and the governed agent loop (Sense → Interpret → Propose → Authorize → Execute → Verify → Learn) enabling unbounded intelligence with bounded execution.
- **The Quantum Reputation System:** A multidimensional, contextual, earned reputation derived from a participant's Catalyst Network and Privacy Networks, accruing along three complementary dimensions (contribution reputation, identity reputation, behavioral reputation). Novel aspects: the Referral/Endorsement distinction (Referrals provide access without staking reputation; Endorsements provide access plus reputation-backed attestation with accountability for failed endorsements), the self-enforcing accountability mechanism (failed endorsements degrade behavioral reputation through the contribution graph without centralized adjudication), and the preferential attachment dynamic where high-reputation participants attract network formation activity through credibility rather than system-assigned privilege.
- **The Catalyst Network Architecture:** A hierarchical network-of-networks contribution graph model (Personal Catalyst Network, Enterprise Catalyst Network, Accelerator Catalyst Network, Quantum Privacy Catalyst Network) where each participant grows a tangible, portable graph asset rooted in their Quantum Privacy Cells. Novel aspects: the parallel structure to Privacy Networks (Privacy Networks govern rights; Catalyst Networks govern contribution and reputation), enterprise graph densification through work-related employee contribution aggregation with visibility-setting-controlled boundaries, and the "Grow your Catalyst Network" activation model where each contribution extends the participant's graph asset independently of settlement timing.
- **The Permanent Privacy Seal:** A coercion-resistant privacy mechanism where contribution records are cryptographically locked such that they are accessible only to automated, Proof-of-Trust Accredited systems and cannot be accessed, viewed, decrypted, or disclosed by any human party — including the contributor, administrators, or any governance authority. Novel aspects: irreversible seal application eliminating the possibility of future reversal under duress, continued graph assembly and settlement function for sealed records (the contributor receives full economic benefit without access to the underlying records), and the coercion-proof design principle (a contributor who has sealed their records can truthfully state that no human possesses the ability to produce them).
- **Privacy Domain-Anchored Rewards Analysis:** A privacy-preserving contribution analysis model where contributors optionally submit contribution content via one-way Privacy Pipes to a QP Rewards service anchored in a Quantum Privacy Domain. Novel aspects: hash validation against the Contribution Ledger confirming authenticity prior to semantic analysis, full semantic analysis within the Privacy Domain boundary producing more accurate chain linkage, cascade attribution, and settlement allocation than metadata-only

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

assembly, with only reward allocations crossing the Privacy Domain boundary — and cross-enterprise chain validation where multiple contributors' contributions enter via separate Privacy Pipes, are validated and attributed within the boundary, and only resulting reward allocations emerge.

B.2 System Architecture Reference: The Quantum Privacy Sidecar Pattern

The Catalyst operates as a local or API-level observer that does not sit in the critical path of the primary work but "witnesses" it. The architecture comprises four client components operating within the three-plane architecture (Data Plane for intelligence, Control Plane for governance, Management Plane for configuration):

- **Client-Side Agent (The Witness):** A lightweight plugin, web application, or API endpoint that captures contribution events through five Signal Input Modes. In Active Mode, the Witness receives direct human input — voice narrations (transcribed via browser speech recognition), pasted text, uploaded documents, or structured form entries — and processes them through the AI Evaluation Pipeline (Contribution Ingestor) to extract structured attribution records including contributor identification, contribution type classification, contact and organization matching, topic extraction, and chain connection detection. In Directed Mode, the Witness receives signals routed through existing workflows (CC'd emails, tagged messages, forwarded meeting summaries) and extracts structured records from them. In Ambient Mode, the Witness monitors authorized sources with per-contributor opt-in and proposes contribution records when it detects contribution-worthy activity. In Institutional Mode, the Witness processes institutional data stores retrospectively at enterprise scale. In Evangelized Mode, the Witness tracks attribution through distribution pathways (EasyAccess Links, referral chains) and records the downstream contribution graphs that distribution generates. For artifact-generating capture (code commits, document signatures, communication events), the Witness has read access only to the specific process memory or file buffer required to calculate the hash — no raw text, source code, or document content is ever transmitted. All Witness operations flow through the Control Plane's Authorization Server before execution; no contribution record is minted without governance authorization.
- **Listener Agent (The Validator):** An asynchronous service that monitors communication channels via API for Proof of Engagement — replies, thread updates, document completions — to validate pending outreach and document claims. The Validator upgrades record status from SENT to VERIFIED_ENGAGEMENT upon detecting valid engagement signals. The Validator also monitors Evangelized Mode distribution pathways for downstream enrollment and contribution events, linking them back to the originating evangelizer's attribution chain.
- **Local QPC Storage (The Vault):** A local, encrypted storage volume where the contributor holds pending attribution records, encrypted with their QPC key. The Vault is the first persistence layer; records are replicated to additional substrates based on the configured Persistence Router strategy. Contribution records are stored as Contribution Verifiable Credentials (fact records) wrapped inside Trust Block Verifiable Credentials (governance envelopes) — the inner signature attesting to content, the outer signature attesting to governance context. Every record is fingerprinted using SHA-256 from a deterministic JSON serialization of receipt-relevant fields, enabling independent tamper detection by any party.
- **Verification Bridge (The Notary):** A server-side listener that accepts third-party confirmations (cross-verification responses, enterprise system corroborations, manager

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

attestations, Endorsement validations) to validate the integrity of locally stored records. The Bridge adds counterparty-originating evidence to the attribution confidence hierarchy without ever requiring the counterparty to disclose their own record contents. The Bridge also processes Referral and Endorsement acknowledgments, updating chain linkages and Quantum Reputation signals when referred or endorsed participants take action.

Every confirmed contribution generates a Contribution Receipt — a SHA-256 fingerprint computed from deterministic JSON serialization of receipt-relevant fields (contributor, contact, organization, contribution type, timestamps, evidence, visibility). Receipt verification produces one of three states: verified (hash matches current data), unverified (no hash provided), or mismatch (data has been modified). Receipts are downloadable as PDF with embedded QR codes encoding the verification URL, providing contributors with immediate, tangible, independently verifiable confirmation that their contribution has been recorded.

B.3 Catalyst Modules

Eight Catalyst Modules operate across five Signal Input Modes (Active, Directed, Ambient, Institutional, Evangelized), each tailored to a specific content domain and interaction pattern. For artifact-generating contributions (code, documents, communications), modules hash work products without extracting content, sign the hash with the contributor's QPC key, and store the resulting attribution record locally. For narrated and relationship-intensive contributions, modules process human input through the AI Evaluation Pipeline to extract structured attribution records. All eight modules feed the same classification pipeline and produce identical Attribution Records stored in the contributor's .qpn archive.

WebVector (General-Purpose Capture & Administration Platform)

- **Target:** All modern browsers (mobile and desktop). API-first architecture enables future distribution through Catalyst Assistant (browser extension), Claude Cowork Plugin, ChatGPT Connector, and MCP clients.
- **Trigger:** Contributor-initiated recording through four Active Mode input methods, or agent-initiated proposals through Directed, Ambient, Institutional, and Evangelized Modes as they activate in later phases.
- **Process:** Four Active Mode input methods — Voice (browser speech recognition with real-time transcription), Paste (clipboard text for LLM extraction), Upload (PDF/DOCX/TXT with server-side text extraction, SHA-256 hashing, and auto-evidence attachment with rule-based strength classification), and Manual (direct structured form entry) — all feeding the AI Evaluation Pipeline for semantic classification, identity enrichment, and entity resolution. A progressive disclosure recording flow (three-step wizard: Extract → Confirm → Receipt) guides the contributor through AI-extracted field review, evidence attachment, visibility selection, and confirmation, completing in under 60 seconds. Email intake extends capture to Directed Mode (CC the Catalyst agent on any outgoing email). Every confirmed contribution generates a SHA-256 fingerprinted Contribution Receipt with tamper detection, downloadable as PDF with embedded QR code.
- **Additional Capabilities:** Contributor portfolio and reputation dashboards (Quantum Reputation signals, attribution readiness, network role classification), proximity-based objective navigation (4-tier relevance scoring with gap guidance and deep links), contribution chain graph visualization (interactive directed graph with shadow nodes for privacy-preserving topology display), program and objective management (admin dual-view with goal rules, contribution-to-objective linking, and contribution-to-contribution linking with typed edges), and behavioral activation system (10 levels, 24 badges, dual XP streams, evidence bonus, streak multiplier, daily cap).

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Privacy:** All AI processing occurs within the contributor's browser session or server-side within the Catalyst application's security perimeter. No contribution content is transmitted to any third party. Visibility is contributor-controlled across four tiers (Confidential, Program, Accelerator, Network). Confidential contributions are never visible to administrators.
- **Architectural Role:** WebVector is the hub from which specialized Vectors extend — incorporating VoiceVector, DocVector, and CommVector (email intake) capabilities in its initial deployment. The QPN Catalyst application is the first WebVector embodiment. It also serves as the administrative portal through which Accelerator Managers operate programs, link contributions to objectives, monitor Quantum Reputation metrics, and oversee contribution graph formation.

CodeVector (DevOps & Engineering)

- **Target:** GitHub, GitLab, Bitbucket, VS Code, JetBrains IDEs (IntelliJ, PyCharm, WebStorm), Xcode, and any Git-compatible version control system.
- **Trigger:** git commit / push, pull request creation or merge, CI/CD pipeline completion, release tag, or contributor-initiated checkpoint.
- **Process:** SHA-256 hash of staged diff content; hash signed with QPC key; record stored locally in .qpn archive; optionally injected into commit trailer as X-QPN-Attribution header. For pull requests, the AI Evaluation Pipeline classifies the contribution type (new feature, bug fix, infrastructure, documentation, security hardening, test coverage) and detects chain relationships to upstream requirements and downstream deployments. CI/CD pipeline completions generate automated deployment confirmation records that upgrade contribution status from CODE_COMMITTED to CODE_DEPLOYED.
- **Privacy:** Actual source code never leaves the contributor's machine — only the hash is transmitted. Enterprise DLP compatible by construction. Repository names, branch names, and file paths are redacted to opaque tokens in the attribution record; only the classification metadata (contribution type, language, complexity estimate, chain indicators) is stored.
- **What CodeVector Captures:** New feature implementations, architectural contributions, security hardening, performance optimization, test infrastructure, CI/CD pipeline development, code review activity, documentation authorship, open-source contributions to QPN ecosystem components, and adapter/connector development for the Enabling Services. Contributions that produce reusable components deployed across multiple Exchange Networks earn enhanced Quantum Privacy Rewards under the Sharing Premium.
- **Architectural Role:** CodeVector is the primary capture module for the Race to Deploy — every adapter, connector, and platform integration described in Section 3.3 flows through CodeVector. The first team to publish a high-quality connector for any given platform captures the Quantum Privacy Rewards for every downstream settlement event that connector enables.

DocVector (Legal & Partnerships)

- **Target:** DocuSign, Adobe Acrobat Sign, Dropbox Sign, PandaDoc, HelloSign, and any document management or e-signature platform accessible via API. Also supports direct document upload through WebVector for platforms without API integration.
- **Trigger:** Envelope creation, signature request event, document completion webhook, or contributor-initiated upload of a signed document.
- **Process:** Hashes PDF binary at signing time; generates opaque Catalyst ID; injects as hidden EnvelopeCustomField where platform supports it; Listener Agent monitors for

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

EnvelopeCompleted webhook to upgrade record status from DOCUMENT_SENT to DOCUMENT_SIGNED. For uploaded documents, server-side text extraction and LLM-assisted field parsing identify the contribution type (partnership agreement, MOU, LOI, teaming agreement, licensing agreement, governance framework, trust authority specification), counterparties, commercial terms, and chain relationships to prior contributions. Evidence is auto-attached with SHA-256 hash and rule-based strength classification (PDF/DOCX → medium; signed agreements with counterparty identification → strong).

- **Native Privacy Network Signing**: In addition to third-party e-signature platform integration, DocVector supports native Privacy Network-enabled document signing — where contributors and counterparties sign documents directly through their QPC keys, producing Trust Block-wrapped Verifiable Credentials with stronger provenance than commercial e-signature services at zero cost. Designed for commercial, legal, governance, and trust-framework contributions that produce formal documentation
- **Privacy:** Document content never transmitted — only the hash and opaque Catalyst ID. For uploaded documents processed through the AI Evaluation Pipeline, text extraction occurs within the Catalyst application's security perimeter; extracted structured fields (contribution type, counterparty organization as opaque token, document category) are stored in the attribution record but the document content itself is not retained beyond the extraction session.
- **What DocVector Captures:** Signed partnership agreements, MOUs, LOIs, teaming agreements, licensing agreements, data sharing agreements, governance frameworks, trust authority specifications, compliance certifications, regulatory filings, and any formal work product that constitutes a verifiable institutional commitment or governance contribution. These are among the most heavily weighted Institutional Activation Milestones in the Quantum Privacy Rewards framework.
- **Architectural Role:** DocVector captures the documentary evidence of commitments that the other modules initiate — an introduction captured by CommVector or VoiceVector that leads to a signed agreement captured by DocVector creates a complete chain from first contact to institutional activation, with each link independently verifiable.

AgentVector (AI & Research)

- **Target:** Claude Code, OpenAI Codex, ChatGPT, Microsoft Copilot, Gemini, Grok, and any AI tool accessible via API, MCP, or session export. Also supports Catalyst Assistant (browser extension) and Claude Cowork Plugin for in-tool capture.
- **Trigger:** Session end, user-initiated checkpoint, or — in Ambient Mode — agent-detected completion of a contribution-worthy AI-assisted workflow.
- **Process:** Hashes interaction logs (prompt + completion metadata); generates Proof of Orchestration verifying the contributor guided the AI to a specific, verifiable outcome (algorithm design, architecture specification, compliance mapping, integration documentation, research analysis, strategy development). The AI Evaluation Pipeline classifies the contribution against the canonical taxonomy, records semantic contribution classification and cascade indicators, and extracts identity attributes for any persons or organizations referenced in the session output. For multi-session research workflows, cross-session cascade detection links related sessions into a unified contribution chain using the Contributor Context Profile (CCP).
- **Privacy:** Raw prompts and AI completions are never transmitted or stored beyond the contributor's session. Only the hash of the interaction log, the classification output, and anonymized entity metadata are retained in the attribution record. The Proof of

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Orchestration attests that the contributor directed the AI to produce a specific outcome without revealing the prompts, intermediate reasoning, or model internals used to reach that outcome.

- **What AgentVector Captures:** AI-assisted research findings, architecture specifications, compliance framework development, strategy documents, model evaluations, algorithm designs, trust taxonomy authorship, data analysis, policy drafts, and any knowledge work product where the contributor's primary contribution is orchestrating AI tools toward a verifiable outcome. As AI-assisted development accelerates across the ecosystem, AgentVector captures the growing category of contributions where the human's value lies in direction, judgment, and orchestration rather than manual execution.
- **Architectural Role:** AgentVector operates primarily in Ambient Mode during later agentic evolution phases (Phases 5–6), where the agent monitors authorized AI platforms and proposes attribution records when it detects contribution-worthy activity. In earlier phases, it operates through Active Mode (contributor exports session output) and Directed Mode (contributor sends session summary to the Catalyst agent). The governed agent loop ensures that all Ambient Mode proposals require explicit human approval before any attribution record is created.

CommVector (Outreach, Advocacy & Engagement)

- **Target**: Gmail, Outlook, Slack, LinkedIn, iMessage, WhatsApp, Signal, Telegram, SMS.
- **Real-Time Verified Loop:** Hash formula: H(Body_Text + Recipient_Domain + ISO8601_Timestamp). Message-ID captured for matching. Listener Agent polls the sending platform’s API for In-Reply-To or thread_ts references matching the captured Message-ID. Upon valid reply detection: record status upgrades from SENT to VERIFIED_ENGAGEMENT; reply metadata appended (timestamp, thread depth, reply domain); cascade indicator updated based on reply content classification.
- **Retrospective Archaeology:** The contributor exports their full communication archive to a secure local environment. The AI Evaluation Pipeline’s semantic evaluation stage performs full-archive analysis — not keyword filtering, but causal-enablement intent assessment — to identify contributions that meet the taxonomy criteria. For each qualifying interaction, a retroactive Trust Block is generated and signed by the local AI agent acting as a Proof-of-Analysis attestor. Example: A CEO introduction email sent 18 months ago that led to an enterprise pilot commitment is retroactively captured as an Executive Access contribution with a Cascade indicator pointing to the pilot implementation downstream.
- **Privacy Controls:** All PII in CommVector records is redacted to opaque tokens before any transmission or sharing. Example redaction: “Had a call with Sarah Chen at Google” → “Had a call with contact_hash_8f9a at org_hash_2c71.” The zero-knowledge certificate format proves the contributor sent a message with qualifying characteristics (organizational level, outreach intent, domain) without revealing the content, recipient name, or employer.
- **Inbound Email Capture (CommVector Extension)**: The simplest path from a sent email to a contribution record requires no plugin, no browser extension, and no app installation. The contributor CCs or BCCs a QPN Catalyst capture address on any outgoing message. The system receives the email, processes it through the AI Evaluation Pipeline, and generates a draft attribution record for the contributor to confirm via the app or a reply link. This extends CommVector’s reach to any email client on any device — including mobile, webmail, and enterprise clients behind DLP controls that block plugin installation.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Capture address formats:** Each contributor is assigned a personal capture address (e.g., jh-a8f3@log.catalyst.qpn) that routes exclusively to their QPC. Accelerator Managers may provision program-scoped addresses (e.g., lokahi@log.catalyst.qpn) that attribute inbound messages to the program's contribution graph without exposing an individual contributor's identity. Both address types accept email, attachments, and forwarded threads.
- **Attachment processing:** PDF, Word, and image attachments are processed by the AI Evaluation Pipeline alongside the email body. An MOU forwarded as a PDF attachment generates both a CommVector contribution record (for the outreach) and a DocVector-equivalent contribution record (for the signed agreement) from a single CC. Evidence from attachments is hashed and linked to the contribution record, immediately qualifying for the Evidence Bonus in the XP layer.
- **Inbound Email Privacy:** The capture address is known only to the contributor. Recipients on the original email see only the contributor's own email address in the CC field — the capture address is a BCC or is added by the contributor's email client as a silent forward rule. No counterparty is ever aware that a contribution record is being created. All D.3 privacy controls (PII redaction to opaque tokens) apply identically to inbound email content.

MeetVector (Virtual Meetings & Transcription)

- **MeetVector Target**: Virtual meeting platforms (Zoom, Microsoft Teams, Google Meet, Webex, GoTo Meeting, Slack Huddles) and standalone AI meeting intelligence tools (Read.ai, Fireflies.ai, Otter.ai, MeetJamie.ai, Avoma, Fathom, Grain).
- **MeetVector Trigger**: Meeting end or on-demand checkpoint during a session.
- **MeetVector Process**: The MeetVector agent monitors for completed meeting recordings and AI-generated transcripts, hashes the transcript content and meeting metadata, and — where end-to-end native integration is available — automatically classifies contributions and stores attribution records without contributor action.
- **MeetVector Privacy**: Raw transcript text never leaves the contributor's environment. Only the hash, classification output, and anonymized entity metadata are transmitted.
- **Why Meetings Are a First-Class Contribution Surface:** The most strategically consequential contributions to a network effect do not happen in pull requests or DocuSign envelopes — they happen in meetings. An executive decision to commit organizational resources, a technical validation of an architectural approach, a multi-stakeholder alignment that unlocks a pilot, a verbal introduction that sets the cascade in motion: all of these events occur in calls and meetings that currently leave no verifiable, attributable record in any contribution graph.

  The proliferation of AI-native meeting tools has created a new class of structured, machine-readable evidence that the Catalyst can capture without imposing any additional burden on contributors. When Zoom, Teams, or Google Meet generates an AI transcript, and when Read.ai or Fireflies.ai produces a structured summary with action items and identified speakers, those outputs are rich, timestamped, multi-participant evidence of the exact contribution types the Catalyst is designed to attribute — executive access, internal advocacy, technical validation, ecosystem orchestration, and commercial term negotiation.
- **MeetVector Integration Architecture - Two Pathways:** MeetVector operates through two complementary pathways that can be deployed independently or together:

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Pathway 1 — General-Purpose AI Analysis (Immediate, No Integration Required):** The contributor exports a meeting transcript or AI summary (from any platform) and submits it to their general-purpose AI assistant (Claude, ChatGPT, Gemini, Grok) with the EP3 Contribution Context loaded. The Three-Stage Evaluation Pipeline classifies any qualifying contributions identified in the transcript, generates identity-enriched attribution records for all participants mentioned, and produces a session delta for import into the contributor's .qpn archive. This pathway requires no new software installation — it works with any meeting platform that produces an exportable transcript, and any AI assistant that supports document upload.
- **Pathway 2 — Native Platform Integration (End-to-End Provenance):** The MeetVector agent integrates directly with the meeting platform or AI meeting tool via API. Upon meeting completion, the agent automatically:
  (1) retrieves the transcript and AI-generated summary;
  (2) hashes the full transcript using the Attribution Record schema;
  (3) runs the AI Evaluation Pipeline against the structured content;
  (4) generates attribution records for each identified contribution event;
  (5) stores records in the contributor's .qpn archive and replicates to configured persistence substrates; and
  (6) optionally notifies identified participants of their contribution records and invites cross-verification. This pathway provides end-to-end cryptographic provenance — the contribution record is signed at the moment the transcript is produced, before any human editing or curation, establishing an unbroken chain from the meeting event to the attribution record to the eventual Quantum Privacy Rewards settlement.

- **What MeetVector Captures:** From a transcript or AI summary, The AI Evaluation Pipeline identifies and attributes the following contribution types:
  - **Executive Access & Introduction:** A meeting in which a contributor introduces a C-suite decision-maker to QPN/PNX leadership, or facilitates a high-level strategic briefing. Speaker attribution identifies who made the introduction; participant identity enrichment captures organizational roles.
  - **Internal Advocacy & Facilitation:** An internal enterprise meeting in which a contributor presents QPN/PNX to colleagues, briefs leadership, or builds internal consensus for adoption. The transcript serves as evidence of the advocacy activity; the participant list establishes organizational reach.
  - **Technical & Compliance Validation:** A technical review, architecture walkthrough, or compliance assessment meeting. The AI-generated summary of key findings and decisions becomes the evidence base for a Technical Validation contribution record.
  - **Ecosystem Orchestration:** A multi-party coordination meeting in which a contributor facilitates connections between participants, structures joint ventures, or brokers resource pool or Exchange Network agreements. MeetVector captures the facilitator's orchestration role even when that role is invisible in written artifacts.
  - **Commercial Term Negotiation:** A meeting in which commercial terms for resource provider agreements, Exchange Network participation, or Trust Block conditions are discussed or agreed. AI-generated meeting summaries that capture "agreed to move forward on X terms" or "committed to Y by Z date" are classified as commercial orchestration contributions.
  - **Commitment Capture & Follow-Up Attribution:** AI meeting tools extract action items and commitments ("John will send the pilot proposal by Friday", "the team agreed to

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

proceed with the integration"). MeetVector records these as pending contribution records with a COMMITMENT_STATED status, which upgrades to COMMITMENT_VERIFIED when the downstream action (a DocVector-captured agreement, a CodeVector-captured commit, a CommVector-verified follow-up) is observed. This creates a verifiable chain from verbal commitment to executed action — the most powerful cascade attribution evidence available.

- **MeetVector Target Platforms & Integration Mechanisms:**
  - **Virtual Meeting Platforms (Native Integration via API or Bot):** Zoom (Zoom Apps SDK, Meeting Bot API, transcript webhook), Microsoft Teams (Graph API, Teams App, transcript and recording events), Google Meet (Google Workspace Events API, Meet Add-On), Webex (Bot Framework, xAPI, transcript access), GoTo Meeting (Meeting API), Slack Huddles (Slack API, transcript capture). Integration mechanism: post-meeting webhook delivers transcript and metadata to MeetVector agent; alternatively, a Meeting Bot participant joins the session and captures the transcript in real time.
  - **AI Meeting Intelligence Tools (Direct Integration via API):** Read.ai (API access to meeting summaries, action items, speaker insights), Fireflies.ai (Fireflies API, structured transcript and topic extraction, CRM sync), Otter.ai (Otter API, live transcript, summary export), MeetJamie.ai (summary and action item export), Avoma (Conversation Intelligence API), Fathom (summary export), Grain (highlight and clip API). Integration mechanism: post-meeting API pull retrieves structured summary and transcript; The AI Evaluation Pipeline classification runs against the structured output. Because these tools already perform AI analysis of meetings, MeetVector can consume their enriched outputs rather than re-analyzing raw audio — reducing latency and computation while leveraging the tool's speaker diarization, topic clustering, and action item extraction.
- **MeetVector Privacy Architecture:**
  - **Transcript Handling:** Raw transcript text is processed locally (or within the contributor's enterprise security perimeter in Mode C). The full transcript is never transmitted outside that boundary. Only the SHA-256 hash of the transcript content, the AI Evaluation Pipeline classification output, and anonymized entity metadata (speaker roles, organizational affiliations as opaque tokens) are stored in the attribution record and replicated to persistence substrates.
  - **Multi-Party Consent:** A meeting involves multiple participants who did not explicitly consent to Catalyst attribution at the time of scheduling. MeetVector handles this through a two-tier model:
    (1) the contributor's own contributions (statements they made, introductions they facilitated, commitments they expressed) are attributed to their QPC without requiring counterparty consent — exactly as CommVector attributes outreach to the sender;
    (2) counterparty contributions (statements other participants made that represent attributable contributions) are recorded as pending cross-verification requests using the standard Cross-Verification Protocol (B.7), delivered through the counterparty's preferred channel. Counterparties who confirm are added to the contribution graph; those who do not are retained as anonymous participants whose presence is recorded but whose identity is not attributed.
  - **Meeting Bot Disclosure:** When MeetVector deploys a Meeting Bot participant (Pathway 2, native integration), standard meeting recording consent disclosures apply. The Bot is identified as a QPN Catalyst Observer in the participant list. Participants who do not

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

consent to recording may be excluded from the session; their potential contributions are captured only through the initiating contributor's own account of the meeting content.

- **Permanent Privacy Seal Compatibility:** MeetVector attribution records are fully compatible with the Permanent Privacy Seal mechanism (B.10.3). A contributor who seals their meeting records retains full Quantum Privacy Rewards from those contributions while ensuring that the transcript hash, participant identities, and contribution classifications are accessible only to automated compliance and graph assembly systems — never to human reviewers, managers, or legal process. This is particularly important for contributors whose meeting content involves commercially sensitive negotiations, internal organizational dynamics, or personnel matters.

- **The MeetVector End-to-End Provenance Advantage:**

  When MeetVector is built directly into the meeting platform or AI meeting tool (Pathway 2), the provenance chain is unbroken: the cryptographic hash is computed at the moment the transcript is produced, before any human editing, curation, or selection. This is materially stronger evidence than Pathway 1 (contributor-submitted transcript), because it eliminates the possibility of selective submission — the contributor cannot choose which parts of the meeting to include.

  This creates a strong commercial incentive for meeting platform vendors and AI meeting tool providers to adopt native MeetVector integration: their customers earn higher Quantum Privacy Rewards confidence scores (and therefore higher rewards) when using platforms with end-to-end provenance, compared to platforms that require manual transcript export. Platform vendors who integrate MeetVector natively earn Quantum Privacy Rewards under the Reusable Infrastructure Development category, and their platforms gain a competitive differentiator for every enterprise customer operating within the QPN ecosystem.

VoiceVector (Voice Narrative Capture)

- **VoiceVector Target:** The QPN Catalyst mobile and web app, with keyboard shortcut (Press R) support in desktop environments.
- **VoiceVector Trigger:** Contributor taps the microphone button or presses the designated shortcut and speaks a natural-language description of a contribution event ("What happened?"). Also triggered by the Paste input mode (clipboard text from any source) and the Manual input mode (structured form entry).
- **VoiceVector Process:** The contributor's spoken narration is transcribed in real time and immediately submitted to the Three-Stage AI Evaluation Pipeline. The AI classifies the contribution against the Catalyst Contribution Taxonomy, extracts identity attributes for all referenced contacts and organizations, and produces a pre-populated Review & Confirm screen for the contributor to approve. The contributor may re-record at any time before confirmation. The resulting attribution record is signed with the contributor's QPC key and stored in the local .qpn archive.
- **VoiceVector Privacy:** Audio is processed locally or via a zero-retention speech-to-text API; raw audio is never stored or transmitted after transcription. The transcription is processed as a standard text input to the AI Evaluation Pipeline — no separate audio archive is created.
- **Three VoiceVector Input Modes:** VoiceVector exposes three input modes for contributors who do not have or prefer not to use a technical capture tool (CodeVector, DocVector, AgentVector, CommVector, MeetVector, VoiceVector, MessageVector). All three modes feed the same AI Evaluation Pipeline and produce identical Attribution Records with consistent classifications.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Voice (primary mode):** "What happened? Tap and describe it in your own words." The app provides contextual example prompts (e.g., "Met with Sarah Chen at Meridian Health about using quantum privacy in their patient data system. Her email is sara.chen@meridianhealth.com") to guide contributors toward maximum-attribute capture without requiring them to know the taxonomy. Real-time transcription is displayed during recording; contributors tap to finish. This is the lowest-friction capture method for relationship-intensive contributors whose primary activities are meetings, introductions, and advocacy — exactly the contribution types that carry the highest Launch Premium weights.
- **Paste:** The contributor copies any text — an email thread, a chat excerpt, a meeting note, a calendar entry — to their clipboard and pastes it into the app. The AI Evaluation Pipeline processes the full pasted content using causal-enablement classification, exactly as it would process a CommVector message archive or a MeetVector transcript export. This bridges the gap between contributors who have exportable text evidence but are not using an integrated capture module.
- **Manual:** A structured entry form pre-populated with the contributor's identity from their CCP. The contributor fills in contact name, organization, contribution type, topic, program, and evidence attachment. Manual entries are assigned a lower default confidence score than Voice or Paste entries because the AI has less raw content to evaluate; attaching supporting evidence (a PDF, a screenshot, an email export) upgrades the confidence score at submission.

MessageVector (Universal Messaging Proxy & Attribution Capture Network)

- **MessageVector Target:** Any communication channel — email (any provider or domain), messaging platforms (WhatsApp, Signal, iMessage, Slack, Telegram, SMS), efax services, and physical mail processing services — through a network of privacy-preserving proxy addresses that route inbound communications to QPN Catalyst for AI classification and attribution, without any counterparty ever interacting directly with QPN Catalyst systems.
- **MessageVector Trigger:** Receipt of any inbound message or document at a MessageVector proxy address. No contributor action required beyond the initial proxy setup.
- **MessageVector Process:** Inbound messages are received at proxy addresses, forwarded to the QPN Catalyst processing pipeline via Privacy Pipe or encrypted relay, processed by the AI Evaluation Pipeline for semantic classification, attachment extraction, and entity resolution, and converted to draft Attribution Records. The contributor receives a confirmation notification and approves the record via the QPN Catalyst app or a reply link. Records created through MessageVector proxies are attributed to the contributor who owns the proxy address, or — in the case of referral proxy addresses — to both the proxy owner (as Referral credit) and the message sender (as direct contribution credit, if they are a QPN participant).
- **MessageVector Proxy Address Architecture:** MessageVector operates through a layered proxy network. Each layer serves a different privacy and attribution purpose:
  - **Personal Proxy Address:** A contributor-specific address (e.g., jh-a8f3@log.catalyst.qpn or jh-a8f3@any-domain-the-contributor-controls.com) that routes all inbound messages to the contributor's QPC. The contributor uses this address when they want to capture their own inbound correspondence — replies to outreach, signed agreements sent back to them, or meeting confirmations — without installing any plugin. The address is generated at onboarding and can be added as a silent BCC rule in any email client or as a CC address the contributor habitually includes.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Referral Proxy Address (Custom Attribution Address):** When a contributor invites a contact into the ecosystem, they provision a unique proxy address specifically for that contact — effectively a personalized "contact-specific mailbox." The contributor gives this address to the contact as their preferred communication channel (e.g., "Please use this email for anything related to the Lokahi program"). Any message the contact sends to this address implicitly credits the contributor who provisioned it as a Referral or Introduction contribution, without the contact ever knowing they are interacting with a QPN system. The contact's privacy is fully protected — they see only a normal email address in their own domain or a plausible third-party domain. Attribution of the Referral credit to the proxy-provisioning contributor is automatic and requires no further action.
- **Custom Domain Proxy:** A contributor or organization may configure any email address in a domain they control (personal, enterprise, or third-party) to forward inbound messages to the MessageVector pipeline through one of three connection methods, ordered by increasing privacy protection: direct SMTP forwarding (simplest, destination IP visible in server logs); VPN-tunneled SMTP forwarding (the forwarding connection is encrypted and the QPN Catalyst destination IP is masked from network-level observers such as corporate firewalls and ISP logs — sufficient for most contributors and configurable with any standard VPN provider or WireGuard endpoint); or server-side Privacy Pipe relay (strongest — the forward executes within the server environment through QPN-native encrypted infrastructure, leaving no detectable signal at any network layer, indistinguishable from normal server-side email routing). Contributors behind aggressive enterprise network monitoring should use the Privacy Pipe relay option; contributors operating personal or third-party domains will typically find VPN-tunneled forwarding sufficient. All three methods support MX record redirect as an alternative to explicit forwarding rules.
- **Routing Tokens ("Route To" / "Attention Of"):** For shared program addresses or physical mail processing services, attribution to a specific contributor is established via a routing token embedded in the address or on a physical address label — analogous to "Attention Of: JH-A8F3" on a postal envelope or "Route To: jh-a8f3" as a sub-address (the portion after a + in an email address). This enables a single shared program address to correctly attribute inbound communications to the individual contributor who generated the contact, without requiring a unique address per contributor.

- **MessageVector Channel Coverage:** MessageVector is designed to be channel-agnostic. The processing pipeline is identical regardless of how the message arrives; only the ingest adapter differs by channel.
  - **Email (any provider or custom domain):** Standard SMTP ingest. Supports CC, BCC, forwarding rules, MX record redirect, and server-side Privacy Pipe relay. Handles inline text, HTML, and attachments (PDF, Word, images, spreadsheets). This is the Phase 1 priority channel — universally available, zero client-side installation required.
  - **Messaging platforms (WhatsApp, Signal, iMessage, Slack, Telegram, SMS):** Proxy phone numbers or account addresses that forward message content to the pipeline. Signal and WhatsApp support account-level forwarding through linked device configurations; Slack supports webhook-based channel forwarding. SMS and iMessage proxies use virtual phone numbers (e.g., via Twilio or equivalent) that the contributor provides to contacts as their "project number" or "work line" for a given program. Phase 2 channel.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **eFax:** Virtual fax numbers provisioned per contributor or per program. Inbound faxes are received as PDF images, OCR-processed by the AI Evaluation Pipeline, classified, and converted to Attribution Records. Particularly relevant for healthcare and legal contributors whose counterparties routinely transmit signed documents by fax (MOUs, LOIs, referral agreements, consent forms). Phase 2 channel.
- **Physical mail processing:** Integration with third-party mail scanning and digitization services (e.g., Earth Class Mail, PostScan Mail, or equivalent). The contributor maintains a physical mailbox address — either through the service directly or via a forwarding arrangement — that appears as a normal business or personal address to any sender. Inbound physical mail is opened, scanned, and delivered as PDF images to the MessageVector pipeline; the AI Evaluation Pipeline performs OCR and classification identically to digital channels. Routing tokens on the envelope ("Attention Of: JH-A8F3") or on the address label attribute the record to the correct contributor. This channel is relevant for government relations contributors, senior executives at regulated institutions, and international contributors whose counterparties use physical correspondence as a standard business practice. Phase 3 channel.

- **MessageVector The Referral Proxy: Passive Attribution Without Counterparty Awareness:** The Referral Proxy address is the most strategically significant MessageVector feature. It transforms the act of giving someone a contact address into an automatic, passive attribution mechanism — every message that contact subsequently sends to that address credits the contributor who gave it to them, without any ongoing action required from the contributor and without any awareness on the part of the contact.

  Example: A strategy consultant introduces a health system CTO to the Lokahi program and gives the CTO a custom email address — lokahi-cto-mj@[consultant's domain].com — as the preferred contact for all Lokahi-related correspondence. The consultant's email server forwards all messages received at that address through a server-side Privacy Pipe to the MessageVector pipeline. Every email, document, or signed agreement the CTO subsequently sends to that address — whether an LOI, a pilot proposal, a meeting request, or a signed MOU — generates a contribution record attributed to the consultant (as Referral / Executive Access credit) and, if the CTO is a QPN participant, to the CTO (as a direct contribution). The CTO never interacts with any QPN system. The consultant never needs to remember to record the contribution. The entire attribution chain is built passively, from a single setup action.

  This mechanism directly addresses the most common failure mode of contribution tracking in relationship-intensive networks: the contributor forgets to log the follow-up, the signed document arrives three weeks later and is never associated with the original introduction, and the attribution chain is broken. With a Referral Proxy, the chain cannot be broken — it is maintained automatically by the routing architecture, not by the contributor's memory or discipline.

- **MessageVector Privacy Architecture:** MessageVector's privacy design operates on three principles that are stronger than those of any other capture module:
  - **Counterparty invisibility:** No counterparty ever interacts with a QPN Catalyst system, sees a QPN Catalyst address, or has any indication that their communication is being processed for attribution purposes. To the counterparty, every MessageVector proxy looks like a normal email address, phone number, fax number, or mailing address in a familiar domain.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Traffic analysis resistance:** Server-side Privacy Pipe relay means that even a network observer monitoring the contributor's email server traffic cannot determine that messages are being forwarded to QPN Catalyst — the forward is executed within the server environment, below the level of any client-side monitoring tool, DLP system, or network proxy. Contributors who work at enterprises with aggressive email monitoring can operate MessageVector without any detectable signal on the enterprise network.
- **Compliance screening and fraud prevention:** All inbound messages are processed through the same Privacy-Preserving Compliance Service (PPCS) and Financial Crime and Fraud Prevention Service (FCFPS) that govern settlement-stage contribution records. Anomalous patterns — a single proxy address receiving an implausible volume of high-value signed agreements, a routing token being shared across multiple senders, a proxy address receiving communications that do not match the contributor's declared program context — are flagged for Manager review before the corresponding attribution records are activated. The compliance screening layer means that the privacy properties of MessageVector cannot be exploited for fraudulent attribution, money laundering, or other criminal misuse.

- **MessageVector Relationship to Other Catalyst Modules:** MessageVector complements rather than replaces CommVector, MeetVector, and VoiceVector. CommVector captures the contributor's outbound activity from within their email client. MessageVector captures inbound responses and documents routed through proxy addresses, without requiring any email client integration. Together, they form a complete inbound-outbound attribution loop for email-based relationship work. MeetVector captures what is said in meetings; MessageVector captures what is sent before and after. VoiceVector captures what the contributor narrates; MessageVector captures what the counterparty independently transmits.

  A document received via a MessageVector eFax proxy is processed identically to a document uploaded through VoiceVector's Manual input mode or attached to a CommVector-captured outreach thread — the same AI Evaluation Pipeline, the same Attribution Record schema, the same Evidence Bonus in the XP layer, and the same confidence upgrade pathway through the Cross-Verification Protocol. The channel of delivery is irrelevant to the attribution record; only the content, classification, and provenance chain matter.

B.4 Three-Stage AI Evaluation Pipeline

The AI Evaluation Pipeline is the intelligence layer that transforms raw contribution signals — voice narrations, pasted text, uploaded documents, emails, meeting transcripts, code commits, and AI session outputs — into structured, classified, identity-enriched attribution records. It operates as the core extraction engine within the QPN Catalyst application (processing all Active and Directed Mode inputs) and can be embedded in third-party AI tools, browser extensions, IDE plugins, and enterprise API deployments to extend contribution capture across the contributor's full professional workflow.

The pipeline operates in three sequential stages for each contribution evaluation:

- **Stage 1: Semantic Contribution Classification:** The AI evaluates the work product against the EP3 Contribution Context using causal-enablement logic — not keyword matching. The evaluation assesses whether the contribution meaningfully enabled, advanced, or created the conditions for ecosystem formation across any of the eight primary categories and two supplementary categories. Output: primary category, confidence score (0.0–1.0), cascade

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

indicator, impact estimate (High/Medium/Low/Uncertain), reusability flag, evaluation model, and timestamp.

- **Stage 2: Identity Enrichment & Entity Resolution:** For each person and organization referenced in the contribution, the AI Evaluation Pipeline generates multi-attribute identity anchors using a maximum-attribute-capture-at-minimum-contributor-effort interaction design:
  - The AI auto-populates known attributes from the CCP and the canonical Organization Directory (no re-prompting for previously captured contacts).
  - For new contacts, the AI asks targeted enrichment questions (current title, employer, relevant relationships) integrated naturally into the classification conversation — adding at most 30 seconds of contributor time.
  - Organizational disambiguation is automatic: "Microsoft" resolves to the specific subsidiary, product group, or operating unit based on prior context. Alias support maps common abbreviations, TLAs, and speech-recognition variations to canonical organization names via a configurable domain glossary.
  - Engagement signal detection identifies pre-milestone activity (Meeting Requested, Introduction Requested, Follow-up Sent) and follow-up clarification questions resolve ambiguity when upgrade cues are detected.
  - New attributes are appended to the CCP session delta for export at session end.
- **Stage 3: Temporal Durability Anchoring:** Records are linked to multiple independent identity anchors to ensure claimability across life events. The AI identifies and captures: employment history signals (references to past employers, transition language); social graph markers (mutual connections, organizational affiliations); credential signals (certifications, degrees, professional licenses); and temporal markers (event-linked timestamps, conference references). These anchors ensure that a contribution record attributed to "Dr. Sarah Chen, VP Engineering, Acme Corp, March 2026" remains claimable by its author even after job changes, name changes, or organizational restructuring.

AI Evaluation Pipeline Integration Modes

The AI Evaluation Pipeline operates in four modes depending on the contributor's tool environment:

- **QPN Catalyst Native:** The pipeline runs within the QPN Catalyst application as its core extraction engine. All Active Mode inputs (Voice, Paste, Upload, Manual) and Directed Mode inputs (email intake) are processed through the pipeline server-side. The contributor interacts through the progressive disclosure recording flow (Extract → Confirm → Receipt) with AI-extracted fields pre-populated for review. This is the primary operational mode during Phase 0 and the default for all WebVector-based contribution capture.
- **SuperPrompt:** The EP3 Contribution Context is injected into an external AI session (Claude, ChatGPT, Gemini, Grok) as a system-level prompt. The AI evaluates contributions conversationally as part of a working session. The contributor copies the session delta (a structured JSON block) from the AI's output at session end and imports it into QPN Catalyst. Requires: AI platform with file upload or large context window capability.
- **Browser Extension / IDE Plugin:** The Catalyst Assistant browser extension or IDE plugin automatically captures session context, injects the EP3 Contribution Context, routes classification queries to the local or API-accessible AI model, and captures the session

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

delta automatically. No manual copy-paste required. Requires: Catalyst Assistant plugin installation. Available as Chrome/Edge extension and VS Code/JetBrains plugin.

- **API-Level Integration:** A server-side API for enterprise deployments that accepts work-product metadata and returns classification and entity-resolution enrichment. Integrates with enterprise identity providers (EasyAccess, Active Directory, Okta) for automatic organizational disambiguation, leverages enterprise org charts to resolve subsidiary and reporting-line relationships, and supports bulk retrospective processing for Institutional Mode archive-wide analysis of prior communications and documents. Requires: Enterprise deployment of the AI Evaluation Pipeline API server within the organization's security perimeter.

B.5 Personal Archive, Context Profile & Contributor Intelligence Module

The .qpn Archive

Every contributor maintains a portable, encrypted .qpn archive — a JSON file containing the complete chain of Trust Blocks (hashes, signatures, metadata) for all contribution records across all modules. The archive is digitally signed by the contributor’s QPC key and optionally counter-signed by the local Catalyst Agent to prove non-tampering.

- **Offline Verification:** The archive contains all necessary cryptographic proofs (Merkle proofs or Ed25519 signatures) to be self-verifying. A contributor can present this file to a new employer or Accelerator Manager to prove their track record instantly, without requiring online access to any persistence substrate or analytics service.
- **Interim Bridge:** When new persistence substrates come online, the Catalyst Agent replays the local archive’s records to the new substrate through the standard Persistence Router replay operation, ensuring no early work is lost regardless of the infrastructure evolution path.

The .qpn archive is also the portable data foundation from which Quantum Reputation is derived. The contribution history, chain participation, evidence quality, and identity verification records contained in the archive feed the reputation engine's three-dimension computation (contribution reputation, identity reputation, behavioral reputation). A contributor's Quantum Reputation travels with their archive — portable across employers, Accelerators, and jurisdictions.

The Contributor Context Profile (CCP)

During Phase 0, the QPN Catalyst application implements the core CCP concepts natively — the Organization Directory provides organizational disambiguation and alias resolution, the Contact matching engine auto-populates known contacts, the contribution history and chain graph provide cross-session cascade context, and the proximity engine generates personalized objective recommendations. The portable CCP described below extends these capabilities to external AI tools where QPN Catalyst's server-side intelligence is not available, enabling contributors to carry their relationship intelligence and contribution context into any AI platform.

The Contributor Context Profile is a derived, portable document generated locally from the .qpn archive and loaded into AI sessions to provide historical context. It solves the statefulness problem: without it, each AI session starts from zero, losing accumulated relationship intelligence, classification patterns, and identity enrichment. The CCP contains five sections:

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Contributor Identity Block:** The contributor's own identity anchors, pre-populated from prior sessions. When the CCP is loaded, the AI recognizes the contributor immediately and never re-asks for previously provided attributes. New attributes discovered during the session are appended at session end.
- **Contact Roster:** Every person the contributor has previously referenced, with all previously captured identity attributes. When the contributor discusses a known contact, the AI auto-populates identity attributes without prompting. For new contacts, the AI prompts for enrichment — but only for those not already in the roster. The roster enables proactive relationship intelligence: identifying contacts not recently engaged, flagging contacts whose affiliations may have changed, and highlighting contacts with high cascade potential.
- **Organization Registry:** All previously referenced organizations with full identity attributes. Resolves organizational disambiguation automatically — when the contributor references "Microsoft," the AI knows whether they mean the parent, Azure, or a specific subsidiary based on prior context. Tracks organizational change events (mergers, acquisitions, rebranding, leadership changes) to proactively alert the contributor to new opportunities.
- **Contribution Activity Summary:** An aggregated statistical profile of the contributor's historical contributions by category, time period, Accelerator context, and impact estimate. Enables the AI to recommend contribution opportunities aligned with demonstrated strengths, detect contribution gaps, and improve classification accuracy using historical patterns as a prior.
- **Accelerator Context & Affiliation:** Active Accelerator affiliations, governance domains, and Trust Taxonomy references. The AI tags new contributions to the correct Accelerator context automatically. Contributors active in multiple Accelerators have multi-context profiles.

Proactive Contribution Intelligence

With the CCP loaded, the AI shifts from reactive classification to proactive strategic advice:

- **Contribution Recommendations:** Based on the activity summary, contact roster, and Accelerator context, the AI suggests high-value next actions: follow-ups on engaged contacts, technical assessments for organizations in the pipeline, introductions connecting reusable infrastructure to organizations with matching needs.
- **Cross-Session Cascade Detection:** When the contributor engages with a contact or organization that appeared in a prior contribution record, the AI automatically links the new activity to the prior chain — strengthening cascade attribution across long-cycle enterprise engagements that evolve over months.
- **Contact & Organization Change Alerts:** When the AI detects information suggesting a contact or organization has changed — new job title, different email domain, merger reference — it alerts the contributor and suggests updating the roster. It also flags when organizational changes create new contribution opportunities.
- **Referral & Endorsement Intelligence:** Based on the contributor's Catalyst Network, contact roster, and Quantum Reputation context, the AI identifies opportunities for high-value Referrals and Endorsements — suggesting which contacts to refer to specific Exchange Networks, which proposals to endorse based on demonstrated domain expertise, and which counterparties would benefit from introductions the contributor is uniquely positioned to make. The AI distinguishes between Referral opportunities (where

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

the contributor can provide valuable access without domain-specific evaluation) and Endorsement opportunities (where the contributor's expertise qualifies them to stake their reputation on a quality assessment).

Profile Scoping & Privacy

Contributors generate different CCP variants for different contexts:

- **Full Profile:** All identity anchors, complete roster, full registry, complete activity summary. For trusted personal AI sessions with zero-retention guarantees.
- **Work Profile:** Current employer context only, professional contacts, business-relevant entities. For enterprise AI sessions where DLP applies.
- **Minimal Profile:** Contributor identity block only. For platforms where the contributor wants classification without exposing historical context.
- **Accelerator-Scoped Profile:** Filtered to a specific Accelerator's contributions, contacts, and organizations.

Session-Delta Capture & CCP Lifecycle

At session end, the AI produces a structured session delta — a JSON fragment containing only new or changed CCP fields. In QPN Catalyst Native mode, session deltas are captured and merged automatically as part of the contribution confirmation flow. In Browser Extension mode, the delta is captured and merged automatically. In SuperPrompt mode, the AI formats the delta as a copyable block for manual import. In API-Level mode, deltas are processed server-side and merged programmatically. New attributes are appended; changed attributes are flagged for contributor review; old values are preserved as historical attributes.

AI Platform Considerations

Platform	CCP Loading Options	Recommendations
Claude	Projects (persistent context), file upload, API	Projects are the natural fit — one Project per Accelerator context enables automatic profile scoping and persistent cross-session context.
ChatGPT	Custom Instructions, file upload, GPT config	Custom Instructions too small for full CCP. File upload or custom GPT with embedded context preferred.
Gemini	Gems, workspace context, file upload	Gems well-suited. Workspace integration enables automatic org registry population from Google Workspace contacts.
Grok	System prompt, conversation context	Standard SuperPrompt injection. Monitor context window limits for large rosters.
Copilot	VS Code settings, workspace context	Well-suited for developer profiles. CodeVector auto-enriched from GitHub commit metadata.

B.6 Multi-Substrate Persistence Architecture

The Persistence Adapter Interface

Every persistence substrate implements five core operations: write (persist an encrypted attribution record), query (retrieve all records for a contributor DID), verify (confirm a record exists and is unaltered), healthCheck (substrate availability and latency), and capabilities (substrate metadata: immutability type, jurisdiction, redundancy, cost).

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

The QPN Catalyst application and Catalyst Agent interact exclusively with the Adapter interface — never directly with any substrate. The Persistence Router manages replication for all three ledgers defined in the Catalyst architecture (Contribution Ledger, Authorization Ledger, and — when activated — the Settlement Ledger), applying the configured write strategy independently to each.

The Persistence Router & Write Strategies

The Persistence Router manages multiple active adapters with four configurable write strategies:

- **Write-All (Maximum Resilience):** Every record written to every active adapter. A record survives as long as any single substrate survives. Used for HIGH-impact contributions with CASCADE indicators.
- **Write-N-of-M (Balanced):** Each record written to N of M adapters, selected for maximum substrate diversity. Default strategy. The AI Evaluation Pipeline's semantic contribution classification output drives automatic N selection.
- **Write-Primary-Plus-Backup (Cost-Optimized):** Written to a primary adapter (local .qpn) and asynchronously replicated to one backup. Appropriate for routine contributions.
- **Write-Local-Only (Offline):** Records persist only in the local .qpn archive. Used when no external substrates are available. Queued for replication when connectivity is restored.

Reference Substrate Implementations

Substrate	Immutability	Jurisdiction	Cost / Record	Notes
Hedera (HCS)	Cryptographic	Global (decentralized)	~$0.001	Initial DLT substrate. Mirror Node enables BigQuery analytics for graph assembly.
Local .qpn Archive	Best-effort	Local device	~$0	Immediate, offline-capable, portable. Personal Archive & Contributor Intelligence Module integration. Always the first write target.
PostgreSQL / Cloud DB	Contractual	Configurable	~$0.0001	Enterprise-grade. Full SQL query support for graph analytics.
AWS S3 / Azure Blob / GCS	Contractual	Region-configurable	~$0.00005	Object storage with 11-nines durability. High cost-efficiency for bulk records.
IPFS / Filecoin	Cryptographic	Global (decentralized)	Variable	Content-addressed. No single provider. Appropriate for long-term archival.
Sovereign Data Store	Contractual	Jurisdiction-specific	Variable	Government-operated. Required for sovereign Accelerators with data-residency mandates.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Manager-Hosted Cloud (Phase 0)	Contractual	AWS/Azure/GCP region	Cloud-tier pricing	Operated by QP LLC Managers via Supabase (PostgreSQL) on AWS/Azure/GCP — the current operational substrate for the deployed QPN Catalyst application. Protected by QPCPA NDA and Exhibit B trade-secret provisions. Becomes ManagerHostedAdapter in Phase 1.

Substrate Diversity & Resilience

The Persistence Router evaluates substrate diversity across five dimensions when selecting write targets: technology family (distributed ledger vs. cloud vs. object storage vs. local); operator (decentralized council vs. cloud provider vs. contributor vs. government); jurisdiction (different legal regimes ensure no single government action eliminates all copies); access model (public vs. private vs. personal vs. sovereign); and cost structure (preventing economic consolidation onto a single provider).

Minimum Viable Resilience: Local .qpn archive (immediate, offline, contributor-controlled) plus one external substrate. Additional substrates added as the ecosystem matures and contributor contribution volume justifies the cost.

Migration, Replay & Evolution

When a new substrate is added, existing records are replayed from any current substrate to the new one — no manual migration required. When a substrate is retired, records are migrated before removal. Schema evolution is handled upstream of adapters — adding new fields (AI Evaluation Pipeline extensions, visibility metadata, new premium types) requires no adapter modifications. Substrates can be hot-swapped at runtime without stopping the Catalyst Agent.

The QPN Catalyst application's current Supabase (PostgreSQL) persistence serves as the Phase 0 Manager-Hosted substrate. As the Persistence Adapter interface and Router are implemented in Phase 1, existing records will be replayed from the Manager-Hosted substrate to the contributor's local .qpn archive and any additional substrates the contributor configures — ensuring that all Phase 0 contributions are fully portable from the moment the multi-substrate architecture activates.

B.7 Cross-Verification Protocol

Cross-verification extends the SENT → VERIFIED_ENGAGEMENT status upgrade (originating in CommVector but applicable across all Catalyst Modules) into a bilateral attribution chain where the counterparty actively confirms their role and enters the contribution graph. Cross-verification is one of the primary mechanisms through which participants grow their Catalyst Networks — each confirmed counterparty becomes a new node in the contributor's graph, deepening chain connections and strengthening Quantum Reputation for both parties.

- ### Five-Step Protocol

  (1) Initiator publishes the contribution at VERIFIED_PUBLIC tier, making the contribution's hash and classification visible to the network's verification matching system.

  (2) Verification request delivered to the counterparty via their preferred channel.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

(3) Counterparty responds: confirms, confirms with additions (providing supplementary context), declines (record updated with declined status), or disputes (triggers AI-assisted dispute resolution).

(4) Confirmed counterparty added as a graph node; their QPC linked to the cascade chain. Their subsequent contributions automatically extend the cascade.

(5) Counterparty becomes eligible for Quantum Privacy Rewards on the entire downstream graph — making verification itself a recruitment mechanism that grows both parties' Catalyst Networks. The counterparty may also use the verification interaction to provide a Referral (connecting the contributor to additional contacts without staking reputation) or an Endorsement (attesting to the quality or accuracy of the contribution with reputation backing), further extending the graph and strengthening Quantum Reputation for all participants in the chain.

- **Verification Delivery Channels**

  End-to-end encrypted messaging (iMessage, WhatsApp, Signal, Telegram) is preferred for privacy. Supports platform-native disappearing messages, with initial policies set to: 72 hours for high-sensitivity interactions, 7 days for standard, 30 days for low-sensitivity. Also available via SMS, email, in-platform notification, LinkedIn direct message, and deferred verification (held pending until the counterparty joins the Catalyst Network and identity resolves).

- **Verification Integrity**

  Cross-verification strengthens attribution confidence but is not required for Quantum Privacy Rewards eligibility. Unverified contributions earn attribution based on the contributor's own Capture Tool evidence. Anomalous verification patterns (mutual confirmation rings, rapid confirmations, contacts with no independent contribution history) are flagged for review by the AI-assisted dispute resolution system. Verification patterns also contribute to behavioral reputation — participants who consistently provide accurate, well-evidenced verifications build Quantum Reputation over time, while participants whose verifications are frequently disputed or overturned see their behavioral reputation degrade.

- **Prior-Awareness Clarification**

  When responding to a verification request, the counterparty may acknowledge the outreach while asserting that they were already independently aware of the QPN, the Accelerator opportunity, or the specific engagement context. The counterparty may specify the source and circumstances of their prior awareness (a prior introduction from a different participant, an internal briefing, a conference presentation, an independent research effort, or a direct relationship with QPN leadership). This clarification is recorded as a separate, counterparty-originated Contribution Record within the counterparty's QPC.

  Prior-awareness clarifications are subject to an evidence-weighted confidence model: a clarification with supporting evidence (hashed email thread, meeting record, CommVector-verified outreach from the claimed prior source) receives full attribution weight; a clarification corroborated by the named prior source receives high attribution weight; an unsupported assertion receives reduced weight. Critically, the counterparty's prior-awareness clarification is not disclosed to the initiator who sent the original outreach — protecting the counterparty from social pressure and preserving the confidentiality of their internal information sources.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Counterparty Context Enrichment: Three-Tier Visibility Model**

  Once engaged through cross-verification, counterparties can provide organizational and strategic context that facilitates graph linking, gap analysis, and adoption planning:

  - **AI-Only (default):** Enrichment encrypted so no human — including Accelerator Managers — can view the raw content. Accessible only to AI-powered systems (Global Graph Assembly Engine, the AI Evaluation Pipeline, automated attribution logic) for graph linking, cascade reconstruction, attribution confidence scoring, and Quantum Privacy Rewards allocation. Maximum privacy: the counterparty's sensitive organizational intelligence informs the graph without any human ever reading it.
  - **Manager-Visible:** Counterparty elevates specific enrichment items to MANAGER visibility for strategic coordination, gap analysis, and engagement planning. Manager-Visible enrichment earns an additional attribution premium because it enables informed strategic decisions.
  - **Manager-Visible with Outreach Authorization:** Counterparty authorizes Managers to use specific enrichment items to personalize and route follow-on outreach to other contacts within their organization or network. Highest-value tier — earns the highest attribution premium because it directly accelerates ecosystem formation by enabling targeted, informed outreach that would otherwise require independent discovery.

  The counterparty may change visibility tiers at any time. No enrichment item is ever disclosed to the initiator without the counterparty's explicit, per-item authorization — regardless of visibility tier.

  Enrichment contributions may include: organizational structure and reporting relationships relevant to adoption decision-making; identification of internal champions, skeptics, or decision-makers not yet in the contribution graph; vendor, partner, and customer relationships that represent potential adoption pathways or cascade targets; budget cycles, procurement processes, or regulatory timelines that affect adoption timing; political or bureaucratic dynamics that could accelerate or impede engagement — including guidance on how to navigate them effectively; existing technology infrastructure, data assets, or compliance frameworks that could be published as dual-use PNX resources; and competitive dynamics or market pressures that create urgency for participation.

  Participants who provide high-value context enrichment — particularly organizational navigation guidance, internal relationship mapping, and adoption-pathway identification — earn Quantum Privacy Rewards under the Ecosystem Orchestration and Internal Advocacy contribution categories, with attribution weight indexed to the downstream impact their intelligence enables and the visibility tier at which it is shared. This creates a graduated incentive structure: contributing intelligence at AI-Only earns base credit; elevating to Manager-Visible earns a premium; authorizing outreach use earns the highest premium — rewarding progressively greater willingness to enable ecosystem formation while ensuring that every contributor controls exactly how much they share and with whom.

B.8 Global Contribution Graph Assembly Engine

The Global Graph Assembly Engine is an AI-powered service that systematically combines fragmentary contribution graphs from independent, decentralized participants into a unified global contribution graph — constructing and maintaining the Personal, Enterprise, and Accelerator Catalyst Networks that constitute the Quantum Privacy Catalyst Network. In its standard operating mode, the engine operates on classification metadata, opaque entity

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

identifiers, temporal data, and Accelerator context — never on raw contribution content or decrypted PII. When operating within a Quantum Privacy Domain (see Section 10.7), the engine can additionally process raw contribution content submitted via one-way Privacy Pipes — enabling semantic verification that goes beyond metadata matching, such as confirming that a contributed contract was ultimately executed with modifications, verifying that signatories changed between draft and final versions, or analyzing unstructured documents to identify contribution-worthy content that metadata-only classification would miss. The Privacy Domain boundary ensures that no raw content, intermediate results, or identity information is revealed to any person, organization, or external system regardless of operating mode. Privacy-preserving identity resolution operates continuously within the assembly process, matching opaque identifiers across contributions, detecting when different contributors have referenced the same person or organization, and tracing cascade chains to their origins — without revealing identities to any participant, administrator, or external system (see Section 10.7 for the full privacy architecture).

Five Assembly Mechanisms

- **Fragment Linking:** Identifies structural connections between records in different contributors' local graphs that reference the same person, organization, or cascade chain. Links are established through classification metadata and opaque entity identifiers — not through comparing raw content. A contribution record in Contributor A's graph referencing org_hash_2c71 is linked to Contributor B's record referencing the same org_hash, establishing a structural connection between the two cascade chains.
- **Retrospective Chain Reconstruction:** As new records are added to the global graph, the Assembly Engine re-evaluates all existing chains for linkages that become visible only when additional context is available. A contribution recorded in Month 1 that was classified as "Uncertain" cascade potential is automatically re-linked to a contribution recorded in Month 6 that demonstrates the Month 1 contribution triggered downstream action. Referral and Endorsement records create distinct graph edges — Referrals establish access-linkage connections (the referrer facilitated a connection), while Endorsements establish reputation-staked connections (the endorser attested to quality). Both edge types carry different attribution weights in chain reconstruction.
- **Enterprise Graph Densification:** When an enterprise deploys a Private Accelerator with dual-use integration or activates Institutional Mode, its employees' work-related contributions across all Catalyst Modules are aggregated into an enterprise-dense sub-graph — the Enterprise Catalyst Network — that can be selectively contributed to the global graph under EP3 governance. This dramatically increases graph density in high-value institutional segments. Visibility-setting-controlled boundaries ensure that only contributions the enterprise and its employees have authorized for aggregation are included.
- **Cross-Accelerator Graph Synthesis:** Under EP3 Proof-of-Trust governance, contribution graphs from multiple Shared and Private Accelerators are synthesized into a unified view of the global contribution ecosystem. Cross-Accelerator synthesis identifies cascade chains that cross Accelerator boundaries — a contributor in the Healthcare Accelerator introducing a contact who subsequently joins the Financial Services Accelerator — and distributes Cascade Premium across the full cross-Accelerator chain.
- **Privacy Domain-Anchored Semantic Analysis:** When the necessary Privacy Domain infrastructure is deployed and Proof of Trust Accredited, contributors may optionally submit contribution content via one-way Privacy Pipes to a QP Rewards service anchored

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

in a Quantum Privacy Domain (see Section 10.7). The submitted content is validated against cryptographic hashes in the Contribution Ledger and analyzed semantically to produce more accurate chain linkage, cascade attribution, and settlement allocation than metadata-only assembly can achieve — with only reward allocations crossing the Privacy Domain boundary.

Attribution Confidence Hierarchy

The attribution confidence hierarchy feeds directly into the contribution reputation dimension of Quantum Reputation — higher-confidence contributions strengthen the contributor's Catalyst Network more than lower-confidence records.

Confidence Tier	Evidence Basis	Score Weight
Bilateral Cross-Verification	Both parties confirm with supporting evidence. Counterparty context enriched.	**Highest (1.0)**
Endorsement-Backed Verification	Counterparty confirms with reputation-staked Endorsement attesting to contribution quality.	**Very High (0.90)**
Enterprise System Corroboration	Record corroborated by Private Accelerator enterprise dual-use data.	**High (0.85)**
Multi-Participant Triangulation	Three or more independent records referencing same event/person.	**High (0.80)**
Temporal + Organizational Overlap	Records from different contributors referencing same org/time window.	**Medium (0.65)**
Classification + Context Inference	AI classification confidence high; contextual signals strong; no corroboration.	**Medium (0.50)**
Referral-Linked Claim	Contribution linked through Referral connection (access provided, no quality attestation).	**Medium (0.45)**
Single-Source Claim	No corroboration. Contributor's record only.	**Base (0.30)**

B.9 Settlement Controller

The Settlement Controller automates the linking of contribution records to Exchange Token flows, the calculation of Quantum Privacy Rewards, and the recovery of infrastructure costs through a five-stage pipeline. The Settlement Controller reads exclusively from the Contribution Ledger (verified facts) and writes to the Settlement Ledger (economic valuation) — it never modifies contribution records or governance decisions, maintaining the sacred boundary between factual recording and economic allocation defined in Section 7.6.

- **Stage 1 — Graph Resolution:** The engine queries the global contribution graph to reconstruct contribution lineage, identify cascade chains, and determine each contributor's relative share based on classification, timing, scarcity, downstream impact, and Quantum Reputation signals (contribution, identity, and behavioral dimensions). Referral-linked and Endorsement-backed contributions are weighted according to the Attribution Confidence Hierarchy (see B.8). Compute costs for graph resolution are billed against the administrative allocation of the reward pool.
- **Stage 2 — Compliance Filter:** The Settlement Controller invokes the Privacy-Preserving Compliance Service (PPCS) and Financial Crime and Fraud Prevention Service (FCFPS) to verify contributor eligibility and transactional integrity before any value transfer occurs. Contributors whose records are under Permanent Privacy Seal are processed identically to

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

unsealed records — the compliance services operate as Proof-of-Trust Accredited automated systems with access to sealed content.

- **Stage 3 — Revenue Distribution Waterfall:** PNX-settled revenue is allocated through the protocol-defined waterfall: Exchange Root (7.5% of all PNX-settled value, deducted first) → for Accelerator-incubated activity, 80% to the Participant Pool and 20% to the Accelerator Incentive & Investment Pool; for organic (non-Accelerator) activity, 100% to the Participant Pool. Within each pool, individual contributor allocations are computed from the graph resolution output, with Quantum Privacy Rewards reflecting each contributor's verified share of the settlement value their Catalyst Network generated. A verification fee covering compliance-service and graph-resolution compute costs is deducted from the claimant's gross allocation.
- **Stage 4 — Solvency Guarantee:** The system processes only claims with sufficient value to cover their own processing fees — ensuring mathematical solvency. Claims that do not meet the minimum threshold are queued for batched processing when cumulative value is sufficient.
- **Stage 5 — Privacy Domain-Anchored Settlement (when available):** For contributors who have opted into Privacy Domain-anchored semantic analysis (see Section 10.7), the Settlement Controller operates within the Quantum Privacy Domain to compute allocations using full semantic content — producing more accurate attribution than metadata-only graph resolution. Only the resulting Quantum Privacy Rewards allocations cross the Privacy Domain boundary; the underlying content, intermediate calculations, and attribution reasoning remain sealed within the domain.

Settlement is the moment when Catalyst Network activity converts into economic value — when contribution reputation becomes economically realized. Exchange Tokens and Quantum Privacy Rewards are delivered to the contributor's QPC without revealing the underlying contribution details, settlement calculations, or attribution reasoning to any party. The contributor's Catalyst Network and Quantum Reputation are updated to reflect the settlement, strengthening the downstream settlement value component of their contribution reputation.

Privacy-Preserving Compliance & Financial Integrity

The Compliance Filter integrates two core subsystems of the Unified Trust Model:

The Privacy-Preserving Compliance Service (PPCS) performs automated, continuous verification of fiduciary, employment, contractual, and ethics requirements. The PPCS evaluates contributor eligibility against jurisdictional policy feeds, enterprise ethics rules, and employment restrictions using cryptographic identity proofs, zero-knowledge credentials, and Compliance Graph analysis. It produces only compliance attestations and classification directives — eligible, restricted, requires substitution, or redirect to PBDR — without exposing the underlying personal or proprietary data that informed the determination.

The Financial Crime and Fraud Prevention Service (FCFPS) extends the same privacy-preserving logic to transactional integrity, performing anonymized graph-analysis, zero-knowledge risk scoring, and sanctions screening against applicable global standards including the U.S. Bank Secrecy Act, FinCEN guidelines, FATF Recommendations, and EU Anti-Money Laundering Directives.

When the compliance filter detects a conflict, prohibited interest, or suspicious activity, affected allocations are automatically reclassified as Restricted Derivative Rights (RDRs) and redirected to verified Public-Benefit Derivative Rights (PBDR) pools or to compliant substitute

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

participants — ensuring lawful continuity without halting settlement. All compliance evaluations execute within privacy domains and are recorded as immutable Trust Blocks linked to the governing QPC, providing cryptographic auditability without disclosure.

Accelerator Manager Capabilities

- **Ecosystem Dashboard:** Aggregated view of all MANAGER-tier contributions showing volume, category distribution, cascade progress, verification rates, Quantum Reputation coverage metrics, attribution readiness signals, and gap analysis — identifying contribution categories or organizational segments with insufficient coverage.
- **Strategic Bounty Management:** Create, publish, adjust, and retire bounties linked to Accelerator milestones and Quantum Privacy Rewards allocations.
- **Attribution Validation:** Review contribution claims, cross-verification patterns, Referral and Endorsement activity, and dispute escalations with full evidence chains. Validation outcomes contribute to participants' behavioral reputation — consistently accurate claims strengthen Quantum Reputation, while disputed or overturned claims degrade it.
- **Participant Coordination:** Suggest connections between complementary contributors with strategic context — matching a technical validator with a pilot implementer who needs their specific compliance expertise, for example. Coordination suggestions leverage Quantum Reputation signals to identify high-reputation participants whose Referrals or Endorsements would carry the most weight.
- **Contribution Chain Visualization:** Interactive directed graph views on both contribution detail and objective detail pages, with shadow nodes preserving topology for contributions outside the Manager's visibility scope. Chain graphs enable Managers to trace cascade sequences, identify chain gaps, and prioritize linking activity that would strengthen attribution confidence.
- **Progress Reporting:** Aggregated, anonymized reports for stakeholders showing ecosystem formation metrics without individual identity disclosure.
- **Program & Objective Management:** Create, configure, and manage Programs within the Accelerator — setting contributor visibility, assigning objectives with priority levels (Essential / High Value / Stretch) and target dates, and tracking objective progress against defined goal rules. Goal rules support organization-scoped conditions (organizationIds, organizationMatch: any/all, distinctOrganizations) enabling objectives like "Signed partnerships with at least 3 distinct healthcare organizations." The Objective Linking interface within each Program allows Managers to connect individual contribution records to active objectives, create structured links between contributions (follow-up, outcome of, enabled by, duplicate of), and curate the outcome chains that drive Quantum Reputation signals and the Nearby Opportunities feed. A catch-all "Not sure yet" Program (Contributor Visible: Yes) is automatically provisioned for each Accelerator to capture contributions from onboarding participants who have not yet been assigned to a specific Program.

B.10 Technical Reference Schemas

The data structures implementing the architectural patterns described in this Appendix are defined in the QPN Catalyst reference implementation (see Section 7.6 and B.12). Canonical schemas for Attribution Records, the portable archive format (.qpn), Contribution Bounties, and the Persistence Adapter interface are maintained in the QPN Catalyst codebase and engineering documentation, which serve as the authoritative source for current data models. The schemas evolve as the implementation matures and are not reproduced here to avoid version drift between specification and implementation.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

B.11 Foundational Enabling Services

The following components represent reusable building blocks that enable the safe, governed reuse of existing widely deployed products, standards, and online services within the QPN/PNX architecture. Each component is designed as an adapter, bridge, or overlay that wraps existing enterprise and consumer infrastructure — data catalogs, cloud storage, API gateways, CRM systems, CI/CD pipelines, identity platforms, model registries, messaging services, advertising exchanges, and marketplace platforms — making them capable of participating in PNX settlement, Trust Block governance, and Exchange Token attribution without requiring replacement, migration, or modification of the underlying systems.

These building blocks are deliberately domain-agnostic. A Tokenization & Entitlement Proof Layer developed for healthcare data governance is equally applicable to financial services, government, and defense. An API Gateway Settlement Wrapper deployed for one Accelerator's Exchange Networks can be reused across every Accelerator that routes settlement through API-mediated services. A CRM Publishing Witness integrated with Salesforce serves any Accelerator whose participants manage commercial relationships through that platform. This reusability across disparate application domains is a structural property of the architecture: the components operate at the infrastructure layer (storage, compute, identity, governance, exchange) rather than the application layer, meaning they compose freely across Accelerators, Exchange Networks, and Resource Pools without domain-specific customization.

Development of these components will be crowdsourced with both enterprise and grassroots support through the Quantum Privacy Rewards framework — with enterprises contributing engineering resources, infrastructure access, and domain expertise, and grassroots contributors building adapters, testing integrations, and extending platform coverage through the Race to Deploy (Section 3.3). A focused effort will produce reference implementations for each component, mapped into Unified Trust Model Trust Frameworks and Trust Taxonomies incubated through the Proof of Trust Accreditation Accelerator. These reference implementations serve as governance-verified starting points that any Accelerator can adopt, adapt, and extend — ensuring that the trust, compliance, and interoperability properties required for PNX settlement are inherited rather than rebuilt for each new deployment.

The following sections provide detailed capability descriptions, target platforms, installed bases, and development effort estimates for each of the Foundational Enabling Services.

B.11.1 Unity Catalog & Lakehouse Publishing Bridge

Description

A metadata-to-manifest bridge that leverages existing data governance platforms—Unity Catalog, Snowflake Data Governance, BigQuery Data Catalog, and similar enterprise lakehouse layers—to publish governed datasets, lineage graphs, and policy fingerprints as PNX Resources without moving, copying, or exposing the underlying data. The bridge generates Resource Manifests from existing catalog metadata, creating cryptographic fingerprints of schema structure, column-level lineage, and access-policy configurations. Enterprise IAM remains the execution boundary; the QPN settlement layer operates on manifests and trust attestations, not on data.

Capabilities

- **Schema fingerprinting** — cryptographic hashes of table schemas, column types, and partition structures enable identity and version tracking without data exposure.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Lineage Merkle roots** — hierarchical hash trees encoding upstream-downstream dependencies across datasets, enabling trust inheritance verification and cascade attribution.
- **Policy hashing** — deterministic fingerprints of access-control and governance policies, proving that published resources are governed under specific compliance regimes.
- **Snapshot integrity proofs** — point-in-time attestations of dataset state, supporting audit, regulatory evidence, and time-stamped settlement.
- **Resource Manifest generation** — automatic creation of PNX-publishable manifests from catalog metadata, bridging enterprise governance into Exchange Network economics.

QPN/PNX Implementation Role

Treats governed enterprise datasets as publishable PNX Resources, using existing enterprise IAM and governance layers as the execution boundary. Data remains under enterprise control; the PNX settles economic rights to access, reuse, and derive from it. Critically, the bridge generates cryptographic attestations of the enterprise's existing policy enforcement infrastructure—access controls, classification rules, retention policies, audit configurations—enabling downstream consumers and Trust Block validators to verify that specific governance practices are in force without inspecting or replicating the policies themselves. This allows enterprises to satisfy PNX Trust Criteria by demonstrating that their existing governance meets or exceeds required standards, rather than implementing parallel compliance infrastructure. The result is settlement without data replication, monetization without marketplace dependence, and cross-enterprise coordination through verified governance equivalence rather than governance uniformity.

Incremental QPN Value Add

- **Monetization of governed data without marketplace dependence** — organizations generate settlement value from data assets they already catalog, without listing on third-party exchanges.
- **Governance reuse through cryptographic verification** — existing enterprise policy enforcement infrastructure satisfies PNX Trust Criteria directly, eliminating redundant compliance build-out and enabling cross-enterprise counterparties to verify governance equivalence rather than requiring identical policy implementations.
- **Zero-knowledge attribution** — data contributors receive Exchange Token flows proportional to reuse without exposing content.
- **Cross-enterprise settlement coordination** — enables multi-party analytics and AI training workflows where each data provider retains governance while participating in shared value creation.
- **Cascade tracking across reuse chains** — Resource Derivatives that combine data from multiple catalogs inherit upstream Trust Block lineage, ensuring every contributor is attributed across arbitrarily deep reuse chains.
- **Conversion of static compliance investment into economically productive governance infrastructure** — existing access controls, classification taxonomies, and audit practices become direct inputs to Trust Block validation and settlement eligibility.

Target Users

Data engineers, analytics leads, enterprise architects, data governance officers, chief data officers, and data product managers.

Platforms

Databricks Unity Catalog, Snowflake Data Governance, Google BigQuery Data Catalog, AWS Glue Data Catalog, Azure Purview.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Installed Base

Databricks serves ~10,000+ enterprise customers; Snowflake ~9,000+; BigQuery and AWS Glue span the remaining hyperscaler footprint. Combined lakehouse and data warehouse TAM exceeds 100,000 organizations. Virtually every Global 2000 company operates at least one governed data catalog.

Total Addressable Value Enabled

Global enterprise data assets exceed $20–40 trillion in estimated economic value. Even a conservative 5% activation as governed, reusable PNX Resources implies $1–2 trillion in enabled exchange value. As cross-enterprise AI training and analytics workflows intensify, the publishable fraction grows.

Development Effort & AI Leverage

Prototype	Controlled Beta	GA Release	AI-Automatable
3–5 months	**8–12 months**	**18–24 months**	**50–70%**

AI can generate the bulk of the metadata extraction, schema fingerprinting, and manifest serialization logic. Integration testing against vendor-specific catalog APIs and edge-case handling (schema evolution, partition drift, access-policy versioning) require human engineering. Lineage Merkle tree construction is algorithmically well-defined and highly automatable.

B.11.2 Cloud Object Storage Settlement Overlay

Description

A content-addressed wrapper around cloud object storage services that uses audit logs, event streams, and object metadata to trigger PNX settlement events whenever governed resources are accessed, shared, or derived. The overlay operates at the storage infrastructure layer, requiring no changes to applications consuming the objects. It intercepts or monitors access events, computes content hashes, wraps signed URLs with settlement metadata, and emits usage-based settlement receipts to the PNX.

Target Platforms

AWS S3 (including S3 Access Grants), Azure Blob Storage, Google Cloud Storage, MinIO (on-premises), Backblaze B2

Capabilities

- Object-level content hashing with version-aware attestation
- Access event capture from cloud-native audit logs (CloudTrail, Azure Monitor, Cloud Audit)
- Signed URL wrapping that embeds settlement metadata in presigned access tokens
- Usage-based settlement receipt emission on read, copy, and derive operations
- Bucket-level or prefix-level publishing granularity
- Retroactive settlement reconciliation from historical audit logs

QPN/PNX Implementation Role

Transforms existing cloud storage infrastructure into PNX-settled Resource Pools. Every governed object becomes an economically active PNX Resource without migration, duplication, or vendor-specific marketplace enrollment. Settlement is triggered by access

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

patterns already being logged, making activation nearly frictionless for organizations already using cloud storage with standard audit configurations.

Incremental QPN Value Add

- Conversion of static data assets into economically active, settlement-generating resources
- Zero-friction monetization requiring no application changes or vendor marketplace participation
- No vendor permission required: operates at the customer-controlled infrastructure layer using existing APIs and audit mechanisms
- Retroactive value capture from historical access patterns
- Cross-cloud settlement coordination enabling multi-cloud data strategies with unified economic tracking

Target Users

Systems administrators, DevOps engineers, cloud infrastructure architects, security operations teams, data platform engineers

Existing Installed Base

AWS S3 serves over one million active customers. Azure Blob Storage and Google Cloud Storage operate at comparable scale. MinIO is deployed in tens of thousands of on-premises environments. Collectively, these platforms manage well over 100 exabytes of enterprise data, with annual growth rates exceeding 25%.

Total Addressable Value Enabled

Enterprise cloud storage underpins trillions of dollars in data-driven economic value. Even activating 2% of managed objects as PNX Resources would represent $500 billion to $1 trillion in enabled exchange value. The overlay's frictionless activation model and retroactive settlement capability suggest rapid adoption curves once deployed.

Development Effort Estimate

Functional Prototype / Alpha	Controlled Beta	Generally Available (GA)
2–4 developer-months	**6–9 developer-months**	**12–18 developer-months**

AI Development Contribution

60–75% of code and test generation is feasible. Cloud provider API integration patterns are well-documented and highly amenable to AI code generation. Event parsing, hash computation, and settlement receipt formatting are straightforward. The primary human-intensive work involves audit log schema mapping across providers and edge-case handling for eventually consistent storage systems.

B.11.3 Model Registry Descriptor Layer

Description

A publishing bridge for AI/ML model registries that generates PNX-compatible Resource Descriptors for registered models, including model identity hashes, training provenance pointers, performance validation certificates, license fingerprints, and drift monitoring attestations. The layer enables AI models to participate in PNX settlement as attributable, tradeable, and reusable economic assets without exposing model weights or proprietary training data.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Target Platforms

MLflow, Amazon SageMaker Model Registry, Google Vertex AI Model Registry, HuggingFace Hub, Azure ML Model Catalog, Weights & Biases

Capabilities

- Model identity hashing (architecture + weight fingerprint) with version-aware attestation
- Training provenance pointers linking model identity to dataset lineage and compute attestations
- Performance validation certificates capturing evaluation metrics under standardized conditions
- License fingerprinting mapping model usage rights to Trust Block criteria
- Drift monitoring attestation providing ongoing performance state verification
- Fine-tune and derivative lineage tracking across model evolution chains

QPN/PNX Implementation Role

Turns AI models into attributable, settleable PNX exchange assets. Every model registered in a supported registry can be published with full provenance, enabling cross-enterprise AI reuse under Trust Block governance, model-level attribution across cascade chains, and zero-trust deployment validation. Model creators earn Exchange Tokens whenever their models are accessed, fine-tuned, or incorporated into downstream Resource Derivatives.

Incremental QPN Value Add

- Cross-enterprise AI model reuse with cryptographic attribution and settlement
- Model-level attribution across multi-hop cascade chains, enabling proportional rewards to original researchers and trainers
- Zero-trust deployment validation ensuring models meet Trust Criteria before execution in regulated environments
- Conversion of open-source and enterprise model investments into economically active, settlement-generating assets
- Competitive market for model quality through Quantum Ratings indexed to real-world performance outcomes

Target Users

ML engineers, AI researchers, data science teams, MLOps engineers, AI ethics and governance officers, model risk management teams

Existing Installed Base

MLflow is the most widely deployed open-source ML platform with hundreds of thousands of active deployments. HuggingFace Hub hosts over 500,000 public models with millions of monthly downloads. SageMaker, Vertex AI, and Azure ML collectively serve tens of thousands of enterprise customers. The global ML team population exceeds 100,000 organizations with millions of registered models under active management.

Total Addressable Value Enabled

The economic value of AI models is projected to exceed $10 trillion by 2035 as AI becomes integral to enterprise decision-making, healthcare diagnostics, financial modeling, and autonomous systems. Even publishing 5% of registered models as attributable PNX Resources would enable over $500 billion in exchange value, with strong amplification through derivative chains as models are fine-tuned, combined, and redeployed across domains.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Development Effort Estimate

Functional Prototype / Alpha	Controlled Beta	Generally Available (GA)
4–6 developer-months	**9–12 developer-months**	**18–24 developer-months**

AI Development Contribution

65–80% of code and test automation is feasible. Registry API patterns are well-structured and amenable to AI generation. The primary human-intensive work involves training provenance schema design, cross-registry normalization, and cryptographic attestation pipeline design for model weight fingerprinting.

B.11.4 Postgres / MongoDB Native Extension

Description

A lightweight database extension that enables Trust Block creation and settlement event emission directly from standard database operations. The extension intercepts or augments transactional workflows to produce row-level hash attestations, signed audit logs, and settlement triggers without requiring parallel infrastructure or application-layer changes. For developers and database administrators, publishing to the PNX becomes as natural as writing a query. The QPN Catalyst application's Supabase (PostgreSQL) deployment serves as the first operational instance of this pattern — the Contribution Ledger and Authorization Ledger already operate on PostgreSQL, providing a natural foundation for Trust Block attestation and settlement event emission as the extension matures.

Target Platforms

PostgreSQL (via native extension), MongoDB (via change stream processor), MySQL/MariaDB (via plugin), CockroachDB, Amazon Aurora

Capabilities

- Row-level and document-level hash attestation with configurable granularity
- Native settlement triggers on INSERT, UPDATE, and cross-table JOIN operations
- Signed audit log generation anchored to database transaction IDs
- Trust Block template population from database schema and access control metadata
- Batch attestation for high-throughput operational workloads
- Replication-aware settlement ensuring single attestation across replicated clusters

QPN/PNX Implementation Role

Makes PNX publishing database-native, eliminating the integration gap between operational data stores and economic settlement. Every transactional database becomes a potential PNX Resource Pool publisher. The extension operates at the infrastructure layer, meaning developers and application teams do not need to modify application code to begin generating settlement-eligible attestations.

Incremental QPN Value Add

- No parallel infrastructure required: settlement attestation embedded directly in the database engine
- Immediate integration path into millions of existing production deployments worldwide
- Minimal adoption friction for database administrators already managing operational workloads

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- Conversion of routine database operations into economically active settlement events
- Foundation layer for enterprise dual-use integration, enabling the Global Graph Assembly Engine to densify contribution graphs from existing transactional data

Target Users

Database administrators, backend engineers, platform engineers, DevOps teams, application architects

Existing Installed Base

PostgreSQL is deployed in over 3 million production environments globally and is the most popular enterprise open-source database. MongoDB serves over 40,000 enterprise customers with hundreds of thousands of deployments. MySQL/MariaDB installations number in the millions. Collectively, these platforms power the operational data infrastructure of virtually every enterprise sector.

Total Addressable Value Enabled

Operational databases underpin trillions of dollars in global commerce, logistics, healthcare delivery, financial services, and government operations. Even activating 3% of production database operations as settlement-eligible PNX events would represent over $500 billion in enabled value flow. The extension's near-zero adoption friction and compatibility with existing operational practices suggest strong uptake potential.

Development Effort Estimate

Functional Prototype / Alpha	Controlled Beta	Generally Available (GA)
3–4 developer-months	**6–8 developer-months**	**12–15 developer-months**

AI Development Contribution

70% of code generation and test scaffolding is feasible. Database extension patterns are well-documented, and AI tools are highly effective at generating SQL trigger logic, hash computation routines, and audit log formatters. The human-intensive work involves replication-awareness logic and certification testing across database versions.

B.11.5 API Gateway Settlement Wrapper

Description

Middleware for API gateways that intercepts request/response flows to compute usage fingerprints, meter economic activity, and emit PNX settlement receipts for every governed API call. The wrapper operates transparently at the gateway layer, enabling any API—internal or external—to participate in PNX settlement without modification to upstream services or downstream consumers.

Target Platforms

AWS API Gateway, Azure API Management, Google Cloud Apigee, Kong Gateway, Tyk, MuleSoft Anypoint

Capabilities

- Request fingerprinting with payload-blind hashing (headers, routing, parameters)
- Response attestation linking output provenance to upstream resource chains
- Usage metering with configurable granularity (per-call, per-byte, per-session)
- Settlement event triggers emitted asynchronously to avoid latency impact

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- Trust Block enforcement at the gateway layer (pre-request authorization checks)
- Multi-tenant metering supporting shared API platforms with per-consumer attribution

QPN/PNX Implementation Role

Transforms existing APIs into PNX-settled service resources. Every API call routed through a wrapped gateway generates settlement-eligible usage data, enabling API providers to earn Exchange Tokens proportional to actual consumption without building custom billing infrastructure. The wrapper also enables downstream cascade attribution when API outputs are incorporated into Resource Derivatives.

Incremental QPN Value Add

- Conversion of existing API infrastructure into settlement-generating PNX Resources
- Transparent activation requiring no changes to API consumers or upstream service implementations
- Universal applicability across SaaS platforms, internal microservices, and partner APIs
- Foundation for API-mediated AI agent settlement, where agentic workflows spanning multiple APIs generate settlement chains automatically
- Elimination of bilateral API licensing negotiations through standardized PNX settlement

Target Users

SaaS platform operators, API product managers, platform engineering teams, enterprise integration architects, partner ecosystem managers

Existing Installed Base

Millions of active APIs operate globally, with API traffic growing at 30%+ annually. AWS API Gateway alone processes trillions of requests per month. Kong, Apigee, and Azure API Management collectively serve hundreds of thousands of enterprise deployments. The API economy is the dominant integration pattern for modern software architecture.

Total Addressable Value Enabled

The global API economy is estimated at $2–5 trillion annually and growing rapidly as AI agents, microservices, and cross-organizational integrations proliferate. Even activating 10% of enterprise API traffic for PNX settlement would enable $200–500 billion in traceable, attributable value exchange. The wrapper's transparent deployment model and asynchronous settlement emission minimize adoption barriers.

Development Effort Estimate

Functional Prototype / Alpha	Controlled Beta	Generally Available (GA)
2–3 developer-months	**5–7 developer-months**	**10–14 developer-months**

AI Development Contribution

75–85% of code and test generation is feasible. Gateway middleware patterns are highly standardized, and AI tools excel at generating request interception, hash computation, and async event emission logic. Primary human effort involves latency optimization, multi-tenant attribution correctness, and gateway-specific plugin certification.

B.11.6 CRM & Workflow Publishing Witness

Description

A lightweight integration layer for enterprise CRM and workflow platforms that witnesses commercial transactions, deal progressions, contract executions, and engagement events,

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

generating PNX-compatible attestation records without exposing deal terms, customer identities, or proprietary business data. The witness captures cryptographic hashes of deal-stage transitions, contract metadata fingerprints, and engagement validation signals, creating an auditable chain of commercial activity that feeds settlement and attribution.

Target Platforms

Salesforce (Sales Cloud, Service Cloud, Health Cloud), HubSpot, Microsoft Dynamics 365, ServiceNow, Workday

Capabilities

- Deal-stage hashing capturing progression events without exposing deal values or counterparties
- Contract metadata fingerprinting linking signed agreements to Trust Block criteria
- Engagement validation through meeting, email, and activity attestation
- Workflow milestone hashing for multi-step business processes
- Lead-to-revenue cascade tracking for attribution chain construction
- Cross-platform engagement correlation across CRM and marketing automation systems

QPN/PNX Implementation Role

Transforms enterprise commercial workflows into attributable PNX settlement chains. Every deal progression, contract execution, and customer engagement becomes a settlement-eligible event, enabling the organizations and individuals who create commercial value to be proportionally attributed through Exchange Token settlement. The witness layer is particularly powerful for the Accelerator Catalyst's CommVector module, providing institutional-grade corroboration of outreach and advocacy contributions.

Incremental QPN Value Add

- Economic attribution for commercial relationship management, traditionally an unmonetized activity layer
- Zero-knowledge deal attestation enabling settlement without exposing competitive intelligence
- Cascade tracking from initial outreach through revenue realization, enabling long-chain attribution
- Institutional corroboration source for the Global Graph Assembly Engine, dramatically increasing attribution confidence
- Foundation for enterprise dual-use deployment where existing CRM investment generates PNX settlement returns

Target Users

Sales operations leaders, CRM administrators, revenue operations teams, partnership managers, business development directors, customer success managers

Existing Installed Base

Salesforce serves over 150,000 enterprise customers globally. ServiceNow operates in over 7,000 large enterprises. HubSpot, Dynamics 365, and Workday collectively add hundreds of thousands more. CRM platforms are among the most widely deployed enterprise software categories, embedded in virtually every B2B and B2C commercial organization.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Total Addressable Value Enabled

CRM-managed deal flow globally exceeds $100 trillion annually across all commercial sectors. Even linking 1% of deal-stage activity to PNX settlement chains would represent over $1 trillion in attributable value. The witness layer's non-invasive deployment and zero-knowledge attestation model make it compatible with the most restrictive enterprise data governance policies.

Development Effort Estimate

Functional Prototype / Alpha	Controlled Beta	Generally Available (GA)
4–5 developer-months	**8–10 developer-months**	**16–20 developer-months**

AI Development Contribution

60–75% of code and test automation is feasible. CRM API integration patterns are well-documented. The human-intensive work involves deal-stage mapping across heterogeneous CRM configurations, privacy-preserving hash design for sensitive commercial data, and certification testing within enterprise compliance environments.

B.11.7 CI/CD Build & Artifact Witness

Description

A pipeline integration that witnesses software build processes, deployment events, and artifact registrations within continuous integration and delivery systems. The witness generates PNX-compatible attestation records linking code contributions to production artifacts, infrastructure configurations to deployment outcomes, and build provenance to software supply chain governance. It extends the Accelerator Catalyst's CodeVector module to the full software delivery lifecycle.

Target Platforms

GitHub Actions, GitLab CI/CD, Jenkins, CircleCI, Azure DevOps Pipelines, AWS CodePipeline, Buildkite

Capabilities

- Artifact hashing with build-reproducibility attestation
- Deployment fingerprinting capturing infrastructure state at deployment time
- Software supply chain attestation conforming to SLSA and in-toto frameworks
- Infrastructure-as-code reuse attribution for shared Terraform, Helm, and CloudFormation modules
- Build dependency lineage tracking across multi-stage pipelines
- Automated SBOM (Software Bill of Materials) generation with PNX Resource linkage

QPN/PNX Implementation Role

Extends PNX settlement to the software delivery layer, enabling organizations and individual contributors to earn Exchange Tokens for infrastructure code, deployment configurations, and build artifacts that are reused across Exchange Networks. The witness creates a complete provenance chain from code commit to production deployment, feeding the Global Graph Assembly Engine with high-confidence, machine-verifiable attribution data.

Incremental QPN Value Add

- Infrastructure reuse attribution enabling Exchange Token settlement for shared DevOps assets

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- Software supply chain governance integrated with PNX Trust Block verification
- Automated provenance generation reducing compliance burden for regulated software deployments
- Cascade tracking from infrastructure contribution through application-level value creation
- Foundation for open-source economic sustainability through settlement-based contributor compensation

Target Users

DevOps engineers, platform engineers, site reliability engineers, software supply chain security teams, release managers, open-source maintainers

Existing Installed Base

GitHub Actions is used by millions of repositories. GitLab CI/CD serves over 30 million registered users. Jenkins remains deployed in hundreds of thousands of enterprise environments. Collectively, CI/CD platforms process billions of build and deployment events annually across the global software industry.

Total Addressable Value Enabled

The global software economy exceeds $5 trillion annually. Even publishing 5% of build artifacts and infrastructure configurations as attributable PNX Resources would enable over $250 billion in traceable exchange value. The witness's alignment with existing supply chain governance standards (SLSA, SBOM) provides a natural adoption path through compliance-driven deployment.

Development Effort Estimate

Functional Prototype / Alpha	Controlled Beta	Generally Available (GA)
2–3 developer-months	**5–7 developer-months**	**10–14 developer-months**

AI Development Contribution

75–85% of code and test generation is feasible. CI/CD pipeline integration patterns are highly standardized, and AI tools are exceptionally effective at generating build-step injection, artifact hashing, and attestation formatting logic. Human effort focuses on cross-platform normalization and SLSA compliance verification.

B.11.8 Enterprise Data Catalog Overlay

Description

A governance-to-manifest publishing layer for enterprise data catalog platforms that translates existing catalog metadata, trust criteria, classification tags, and stewardship records into PNX-compatible Resource Manifests. Unlike the Lakehouse Publishing Bridge (B.1), which targets analytical data platforms, this overlay addresses the enterprise metadata management layer—the systems where organizations define, classify, and govern their entire data estate across operational, analytical, and archival tiers.

Target Platforms

Alation, Collibra, Informatica Enterprise Data Catalog, SAP Data Intelligence, IBM Watson Knowledge Catalog

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Capabilities

- Governance-to-manifest publishing translating catalog classifications into PNX Resource attributes
- Trust criteria mapping from enterprise data governance taxonomies to QPN Trust Block specifications
- Cross-Accelerator reuse tagging enabling catalog assets to be discoverable across multiple Exchange Networks
- Stewardship chain attestation linking data governance roles to PNX attribution records
- Automated compliance mapping from enterprise regulatory tags (HIPAA, GDPR, SOX) to Trust Criteria specifications
- Data quality score attestation enabling Quantum Rating integration for published Resources

QPN/PNX Implementation Role

Positions enterprise data catalogs as PNX discovery and governance interfaces, enabling organizations to publish their governed data estate to PNX without building separate discovery or compliance infrastructure. The overlay treats existing data stewardship investments as direct inputs to PNX Trust Block governance, converting compliance cost centers into economically productive governance infrastructure.

Incremental QPN Value Add

- Conversion of enterprise compliance investment into settlement-generating governance infrastructure
- Cross-enterprise data discoverability through PNX without centralized data marketplace dependence
- Stewardship-based attribution enabling data governance professionals to earn Exchange Tokens
- Regulatory compliance acceleration through automated Trust Criteria population
- Foundation for cross-domain Resource Pool formation using existing enterprise classification hierarchies

Target Users

Data stewards, enterprise data governance officers, chief data officers, regulatory compliance teams, enterprise architects, information security officers

Existing Installed Base

Enterprise data catalog platforms span the Global 2000, with Collibra, Alation, and Informatica collectively serving thousands of large enterprises managing millions of governed data assets. The enterprise metadata management market is growing rapidly as regulatory complexity increases globally.

Total Addressable Value Enabled

Enterprise data catalog usage spans the Global 2000 and increasingly the mid-market. The governed data assets cataloged in these systems represent a conservatively estimated $500 billion to $1 trillion in publishable PNX value, with strong amplification potential as cross-enterprise reuse compounds through Resource Derivative chains.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Development Effort Estimate

Functional Prototype / Alpha	Controlled Beta	Generally Available (GA)
5–7 developer-months	10–14 developer-months	18–24 developer-months

AI Development Contribution

50–65% of code and test automation is feasible. Catalog API integration is moderately complex due to vendor-specific data models. The primary human effort involves governance taxonomy mapping, Trust Criteria translation logic, and validation testing within enterprise security environments.

B.11.9 Tokenization & Entitlement Proof Layer

Description

A cryptographic middleware layer that combines deterministic data tokenization with zero-knowledge entitlement proofs, enabling governed resources in highly regulated domains to participate in PNX settlement without exposing protected data elements. The layer intercepts data access requests, replaces sensitive values with deterministic tokens, and generates zero-knowledge proofs that the requester is entitled to access the underlying data under the applicable Trust Block criteria—all without revealing the data itself or the specific entitlement basis.

Target Platforms

Deployed atop enterprise IAM systems (Okta, Azure AD/Entra, Ping Identity), integrated with healthcare data platforms (Epic, Cerner/Oracle Health), financial data systems (Bloomberg, Refinitiv), and government data enclaves

Capabilities

- Deterministic tokenization preserving referential integrity across datasets
- Zero-knowledge entitlement proofs demonstrating access authorization without revealing criteria
- Multi-domain token mapping enabling cross-organizational joins on tokenized identifiers
- Entitlement inheritance verification ensuring Resource Derivative consumers hold valid upstream authorizations
- Audit-ready proof archives for regulatory examination without data exposure
- Hardware Security Module (HSM) integration for enterprise-grade key management

QPN/PNX Implementation Role

Enables the most sensitive and heavily regulated data domains—healthcare, financial services, government, defense—to participate in PNX settlement and cross-organizational AI collaboration without compromising privacy protections or regulatory compliance. This layer is the critical enabler for Quantum Privacy's core promise: governed access without data exposure.

Incremental QPN Value Add

- Unlocking regulated-domain AI collaboration at scale by solving the data-access-without-data-exposure problem
- Enabling cross-organizational research and analytics on tokenized data with full settlement attribution

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- Reducing regulatory compliance cost through automated entitlement verification
- Foundation for healthcare, financial, and government Exchange Networks that require zero-knowledge data governance
- Critical infrastructure for Quantum Privacy Cell activation in regulated domains where data sovereignty is non-negotiable

Target Users

Information security architects, compliance engineers, healthcare IT directors, financial technology teams, government data officers, privacy engineers, cryptographic infrastructure teams

Existing Installed Base

The combined regulated-domain data infrastructure spans healthcare (Epic and Cerner serve the vast majority of U.S. hospital systems), financial services (Bloomberg and Refinitiv serve virtually all institutional finance), and government (federal, state, and international agencies). Enterprise IAM platforms (Okta, Azure AD, Ping Identity) collectively serve hundreds of thousands of organizations.

Total Addressable Value Enabled

Healthcare, financial services, and government data collectively represent a domain with over $20 trillion in economic value that is currently underutilized due to privacy, regulatory, and sovereignty constraints. The Tokenization & Entitlement Proof Layer is the single most important enabler for unlocking this value through PNX settlement while preserving the privacy guarantees that regulators and data subjects require.

Development Effort Estimate

Functional Prototype / Alpha	Controlled Beta	Generally Available (GA)
6–9 developer-months	**12–18 developer-months**	**24–36 developer-months**

AI Development Contribution

40–60% of development is AI-assistable. Cryptographic component design, zero-knowledge proof circuit construction, and HSM integration require significant human cryptographic engineering expertise. AI tools are effective for test generation, tokenization logic, and integration scaffolding. The overall AI leverage is lower than other extensions due to the domain's cryptographic complexity.

B.11.10 Audience Graph & Marketplace Generalization

Description

A generalization layer that adapts identity graph, attribution logic, and audience coordination infrastructure from digital advertising and marketplace ecosystems into PNX-compatible economic coordination primitives. The layer transforms engagement signals, conversion events, and marketplace transactions into settlement-eligible PNX activity, enabling platforms that already manage attention, identity, and transactional matching to serve as PNX Exchange Providers without rebuilding their coordination infrastructure.

Target Platforms

Digital advertising platforms (The Trade Desk, LiveRamp, Google Marketing Platform), marketplace platforms (Shopify, Amazon Marketplace Services, Etsy), engagement platforms (Twilio, Braze, Intercom)

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Capabilities

- Identity graph generalization mapping platform-specific user identifiers to QPN Privacy Network references
- Attribution chain translation converting marketing attribution models to PNX settlement cascades
- Engagement signal normalization standardizing cross-platform interaction events for PNX settlement
- Marketplace transaction witness generating settlement attestations from existing order management systems
- Cross-platform audience coordination enabling privacy-preserving multi-channel settlement
- Consent-aware identity bridging respecting user privacy preferences through QPC-mediated authorization

QPN/PNX Implementation Role

Transforms the economic coordination infrastructure already deployed at scale in advertising and marketplace ecosystems into generalized PNX settlement infrastructure. This extension recognizes that advertising platforms, marketplaces, and engagement systems already solve coordination, matching, and attribution problems at global scale—the Audience Graph & Marketplace Generalization layer redirects these capabilities toward universal economic settlement rather than platform-captive value extraction.

Incremental QPN Value Add

- Conversion of existing advertising and marketplace infrastructure investment into PNX settlement capacity
- Privacy-preserving audience coordination replacing the declining third-party cookie and device ID infrastructure
- Universal consent-based identity bridging through QPC-mediated authorization rather than platform-imposed tracking
- Marketplace economic liberation enabling sellers and creators to participate in PNX settlement independently of platform terms
- Foundation for population-scale PNX onboarding through platforms that already have billions of active users

Target Users

AdTech platform architects, marketplace platform engineers, identity resolution specialists, privacy engineers, data partnership managers, creator economy platform operators

Existing Installed Base

The global digital advertising ecosystem spends approximately $700 billion annually, managed through platforms like The Trade Desk, LiveRamp, and Google Marketing Platform that collectively reach billions of users. Marketplace platforms (Shopify, Amazon Marketplace, Etsy) facilitate trillions of dollars in annual transactions. Engagement platforms (Twilio, Braze) process billions of messages and interactions monthly.

Total Addressable Value Enabled

The global advertising ecosystem represents approximately $1 trillion annually. Marketplace transaction volume exceeds $5 trillion. Generalized to economic coordination across

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

engagement, commerce, and content, the addressable value enabled by this layer reaches $5–20 trillion in global economic flows that could be routed through PNX settlement infrastructure. This extension has the highest amplification potential because it connects individual-level economic agency to protocol-level settlement.

Development Effort Estimate

Functional Prototype / Alpha	Controlled Beta	Generally Available (GA)
8–12 developer-months	**14–20 developer-months**	**24–36 developer-months**

AI Development Contribution

50–70% of development is AI-assistable. Identity graph normalization and attribution logic translation are moderately complex but well-structured for AI assistance. The primary human effort involves consent architecture design, privacy regulation compliance across jurisdictions, and cross-platform identity reconciliation under zero-knowledge constraints.

B.11.11 Personalized Exchange & Dynamic Value-Sharing Engine

Description

An economic decisioning and offer-composition layer that reuses existing real-time bidding, auction, recommendation, dynamic pricing, and personalized offer infrastructure from digital advertising and e-commerce ecosystems—and generalizes it to support personalized pricing, matching, and value sharing for any combination of PNX Resources across any domain.

Where advertising platforms solve the problem “given this user, what ad at what bid creates the most value?” and e-commerce platforms solve “given this buyer, what product at what price optimizes conversion?”, this extension solves the generalized problem: “given this participant’s authorized context, what combination of resources under what terms and value-sharing arrangement creates the most value for all parties?”

The engine operates within Quantum Privacy Domains and under Trust Block governance, ensuring that personalization occurs on authorized attributes without exposing participant identity, preferences, or economic position to counterparties. It composes Solutions from heterogeneous PNX Resources—data, AI models, compute, professional services, infrastructure, certifications, relationships, engagement surfaces—and computes dynamic, personalized pricing that reflects the participant’s context, the contributing resources’ Trust Block terms, reuse history, and real-time supply-demand conditions. Value-sharing settlement is computed simultaneously with pricing, distributing Exchange Tokens across all contributing Resources in a composed Solution proportional to their economic contribution.

This extension connects directly to the QPN’s healthcare provisional patent coverage (Quantum Privacy-Enabled Personalized, Value-Based Exchange for Better Health), which claims systems for adaptive pricing, zero-knowledge bargaining, multi-agent bidding, matching markets, dynamic price-discovery logic, and federated offer-response mechanisms—all executed within QPN-enabled infrastructure. The Personalized Exchange Engine generalizes these healthcare-originated capabilities to every domain served by the PNX.

Target Platforms

- **Real-time bidding and auction infrastructure:** The Trade Desk, Google DV360, Amazon DSP, Xandr (Microsoft), programmatic SSPs (Magnite, PubMatic, Index Exchange).
- **E-commerce personalization and pricing engines:** Amazon Personalize, Shopify Functions, Dynamic Yield (Mastercard), Algolia Recommend, Coveo.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Recommendation and offer composition systems:** Netflix/Spotify-style collaborative filtering engines, enterprise product configurators (Salesforce CPQ, Oracle CPQ, Apttus).
- **Marketplace matching platforms:** Uber/Lyft dispatch optimization, Upwork talent matching, financial order-matching engines (NASDAQ, NYSE Arca).
- **Multi-agent negotiation frameworks:** Emerging AI agent orchestration platforms (LangChain, CrewAI, AutoGen) operating within QPC-bounded Privacy Domains.

Capabilities

- **Real-time multi-resource offer composition** — combines heterogeneous PNX Resources into personalized Solution offers, evaluating millions of possible combinations against participant context, Trust Block constraints, and value-optimization criteria in real time.
- **Privacy-preserving dynamic pricing** — computes personalized pricing using authorized attributes within Quantum Privacy Domains. Pricing reflects participant-specific context without revealing identity or economic position. Adapts the zero-knowledge bargaining mechanisms claimed in the healthcare provisional patent.
- **Multi-party value-sharing computation** — simultaneously computes Exchange Token distribution across all contributing Resources at the moment of pricing. Every participant receives a deterministic allocation based on Trust Block terms, contribution weight, and reuse lineage.
- **Auction and matching market generalization** — adapts programmatic advertising auction mechanics and marketplace matching algorithms to PNX Resource exchange. Multiple Solution Providers may bid; the exchange selects based on value, trust, and governance criteria rather than price alone.
- **Context-adaptive offer routing** — routes offers through Exchange Networks based on encrypted contextual signals without revealing the signals to offer generators.
- **Continuous market clearing and dynamic rebalancing** — operates as a continuous exchange with resource pricing, availability, and value-sharing terms adjusting dynamically.
- **Fairness and governance constraint enforcement** — enforces multi-criteria constraints preventing extractive pricing, discriminatory offers, or governance-violating resource combinations.
- **Settlement-integrated pricing** — pricing and settlement computed as a single atomic operation. The price IS the settlement instruction.

QPN/PNX Implementation Role

This extension is the economic brain of the PNX at the transaction layer. Where other extensions publish resources (B.1–B.9), generalize identity and engagement infrastructure (B.10), and verify governance, this extension determines what gets exchanged, at what price, under what terms, and how value is shared—in real time, at scale, under privacy-preserving governance.

The engine inherits decades of engineering investment in real-time decisioning, auction optimization, recommendation algorithms, and dynamic pricing from the advertising and e-commerce industries. These systems already operate at global scale, processing millions of decisions per second with sub-100-millisecond latency.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

The critical architectural distinction: the QPN version operates within Quantum Privacy Domains under Trust Block governance. The participant's context drives personalization, but identity is never exposed. Resource Providers compete on value and governance quality, not surveillance capacity. Value is shared through Exchange Token settlement, not captured by the intermediary.

Incremental QPN Value Add

- **Generalization of trillion-dollar personalization infrastructure** from advertising and e-commerce to any resource domain—creating personalized exchange where none currently exists.
- **Privacy-preserving personalization structurally superior to surveillance-based models** because it operates on authorized, accurate, contextual data rather than inferred profiles.
- **Automated multi-party value sharing** eliminating bilateral negotiation overhead. Value distribution computed algorithmically at the moment of transaction.
- **Zero-knowledge pricing enabling fair exchange in sensitive domains**—healthcare, pharma, government procurement, financial risk transfer.
- **Continuous market formation for resource types that currently lack liquid markets.**
- **Patent-protected competitive moat** through healthcare provisional claims on adaptive pricing, zero-knowledge bargaining, multi-agent bidding, matching markets, and federated offer-response mechanisms.
- **Foundation for AI agent-mediated exchange**—the transaction-layer infrastructure for the agentic economy.

Target Users

Exchange Network operators, Solution Providers, marketplace platform engineers, AdTech architects, e-commerce personalization engineers, healthcare value-based contracting platforms, financial trading system architects, AI agent developers, CPQ system architects, and pricing science teams.

Existing Installed Base

The global programmatic advertising ecosystem processes over 500 billion real-time bid requests daily. E-commerce recommendation and dynamic pricing engines operate at comparable scale across Amazon, Shopify (millions of merchants), and enterprise CPQ platforms. Financial order-matching engines process trillions in daily volume. The combined installed base represents the most computationally mature exchange technology in existence.

Total Addressable Value Enabled

Global advertising ($1T annually), e-commerce ($6T+), healthcare ($10T+), financial services ($25T+ in intermediated flows). The aggregate addressable value is $10–50 trillion in annual economic activity that could benefit from personalized, trust-verified, privacy-preserving exchange with automated value sharing.

Development Effort Estimate

Prototype / Alpha	Controlled Beta	GA
6–10 developer-months	**12–18 developer-months**	**24–36 developer-months**

AI Development Contribution

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

60–75% of development is AI-assistable. Auction logic, recommendation algorithms, pricing computation, and offer-composition pipelines are well-understood. The primary human effort involves privacy-preserving context routing, multi-party value-sharing settlement computation, and fairness/governance constraint enforcement. Mechanism design expertise is partially but not fully automatable.

B.11.12 Token Platform & Liquidity Infrastructure Bridge

Description

A multi-tier adapter layer that enables the Quantum Privacy Token (QPT) Platform and Quantum Privacy Liquidity Pools to operate on top of existing financial infrastructure—spanning traditional financial systems (TradFi), programmable financial technology platforms (FinTech), decentralized finance protocols (DeFi), payment networks, and consumer financial data access infrastructure—rather than requiring purpose-built financial infrastructure. The bridge maps QPT lifecycle operations (token issuance, transfer, custody, redemption, collateralization, liquidity pool deposit/withdrawal, securitization) onto the APIs, protocols, and operational frameworks of existing financial systems, enabling the PNX to inherit decades of investment in trading, clearing, settlement, custody, market-making, compliance, payments, and liquidity infrastructure.

The bridge implements the multi-substrate, multi-jurisdiction tokenization service provider architecture described in the QPT Classifications document, providing the adapter layer through which Tokenization Service Providers connect to the financial infrastructure required for token operations. It also implements the custodian-gated liquidity model, ensuring that fiat redemption and liquidity events are restricted to regulated custodians with established AML/KYC compliance.

Critically, this extension operates within the QPN/PNX's two-track development model: Track A (adoption and dual-use economics) proceeds independently of token activation, while Track B (token platform activation and liquidity expansion) is sequenced by jurisdiction through this bridge.

The bridge also integrates consumer financial data access infrastructure—open banking APIs, healthcare data APIs, and payroll APIs—enabling individuals to activate Personal Privacy Networks and publish personal financial, health, and employment data as governed PNX Resources without requiring institutional sponsorship. This directly implements the Individual Rights–Driven Adoption principle: billions of individuals already have the legal right and technical ability to authorize access to data that institutions hold about them, and the infrastructure to exercise that right already exists at scale.

Target Platforms

Tier 1 — Traditional Financial Infrastructure (TradFi)

- **Exchange and ATS Platforms** (NYSE, NASDAQ, BATS/Cboe, LSE, SGX);
- **Clearing and Settlement Systems** (DTCC, CLS, Euroclear, LCH);
- **Custodial Infrastructure** (BNY Mellon, State Street, Northern Trust, Fidelity);
- **Transfer Agent Systems** (Computershare, AST Financial, Broadridge).

Tier 2 — Programmable Finance / FinTech & Digital Assets

- **Digital asset exchanges** (Coinbase, Kraken, Gemini, Bitstamp);
- **Tokenization platforms** (Securitize, Polymath/Polymesh, tZERO, Tokeny);
- **Custody-as-a-Service** (Fireblocks, Anchorage Digital, BitGo, Copper);

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Stablecoin infrastructure** (Circle/USDC, Paxos/PYUSD);
- **Palm Promax Investments** (ADGM-regulated, $1.5T in tokenized RWAs).

Tier 3 — Distributed Ledger & DeFi Protocols

- **Hedera Hashgraph:**
  - **Hedera Token Service** (HTS) for native, compliance-embedded token issuance with built-in KYC/AML flags, OFAC compliance, and atomic swap support at ~$0.001/transaction;
  - **Hedera Consensus Service** (HCS) for immutable audit logging;
  - **Asset Tokenization Studio** with ERC-1400 and ERC-3643 (T-REX) support for regulated security token issuance with on-chain identity;
  - **Stablecoin Studio** with proof-of-reserve verification and regulatory compliance (MiCA, STABLE Act, GENIUS Act);
  - **Cross-Chain Connectivity** via Axelar Network (60+ chains including Ethereum, Solana, Arbitrum, XRPL). Production deployments include Archax ($500M+ tokenized MMF assets from BlackRock, State Street, Aberdeen, Legal & General), Swarm (tokenized equities including Apple, Tesla), StegX ($100M+ institutional real estate using ERC-7518/DyCIST), and Wyoming Frontier Stable Token (FRNT)—the first U.S. state-issued stable token. Lloyds Banking Group has completed FX trades using tokenized MMF units and UK gilts on Hedera as collateral. Canary HBAR ETF (HBR) trades on NASDAQ. Shinhan Bank completed multi-jurisdictional stablecoin remittance pilots (Korea-Thailand-Taiwan).
- **Ethereum ecosystem**: EVM-compatible smart contracts on mainnet and L2s (Arbitrum, Optimism, Base, Polygon); Uniswap and Curve for concentrated liquidity AMMs; Aave and Compound for lending and collateralization; MakerDAO for decentralized stablecoin collateralization; ERC-3643 for identity-linked compliant tokens; ERC-7518 (DyCIST) for jurisdiction-aware tokenization. Ethereum mainnet holds ~$70B TVL; stablecoin market cap on Ethereum exceeds $166B.
- **Solana ecosystem**: Jupiter DEX aggregator; Raydium and Orca for high-throughput concentrated liquidity and hybrid AMM/order-book trading; Drift Protocol for perpetual futures; Jito for liquid staking and MEV optimization; native SPL token standard for low-cost operations at 1,000+ TPS. WisdomTree has deployed regulated tokenized funds on Solana. Solana DeFi TVL exceeds $9B.
- **Cross-chain infrastructure**: LayerZero, Wormhole, deBridge, and Axelar for multi-chain portability; Hashport on Hedera for asset bridging. deBridge alone has processed over $10B in cross-chain volume.

Tier 4 — Payment Networks & Value Transfer Rails

- **Card networks** (Visa, Mastercard, American Express) for merchant settlement and consumer payment.
- **Real-time payment systems**: FedNow (U.S. instant payments, launched 2023), RTP Network (The Clearing House), SEPA Instant (Eurozone), UPI (India, 10B+ monthly transactions), Pix (Brazil).
- **Digital wallets** (Apple Pay, Google Pay, Samsung Pay, PayPal/Venmo, Cash App).
- **Merchant acquiring and processing** (Stripe, Adyen, Square/Block, Checkout.com).

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Cross-border payment networks** (SWIFT gpi, Wise, Thunes, Nium).
- **Stablecoin payment rails** (USDC, PYUSD, Hedera-based stablecoins including Wyoming FRNT and Australian Digital Dollar AUDD).

Tier 5 — Consumer FinTech & Open Data Access

- **Open banking aggregators**: Plaid (12,000+ U.S. financial institutions, integrated into Venmo, Robinhood, Chime, Betterment, Acorns; also covering Canada, UK, EU), Yodlee/Envestnet (17,000+ global data sources, serving 17 of top 20 U.S. banks—recently acquired by Symphony Technology Group), MX (AI-powered financial data enrichment and categorization), Finicity/Mastercard (credit and lending-focused aggregation), Akoya (owned by Fidelity and 11 major U.S. banks, API-based standardized data sharing). European open banking: TrueLayer, Tink/Visa, Yapily, Salt Edge, Bankin' (PSD2/Open Banking compliance across thousands of EU and UK institutions).
- **Healthcare data access**: FHIR APIs mandated by the 21st Century Cures Act for patient-directed data access covering 300M+ Americans; CMS Blue Button 2.0 for Medicare beneficiary data; patient portal integrations across Epic, Cerner/Oracle Health, and other EHR platforms; Apple Health and Google Health Connect for consumer health data aggregation.
- **Employment and income data**: Payroll connectivity APIs (Pinwheel, Argyle, Atomic) for verified income, employment history, and payroll-directed deposit switching; IRS transcript APIs for income verification; SSA data access for benefit verification.
- **Government and identity data**: IRS account APIs; state motor vehicle records; credential verification services (education, professional licenses); emerging digital identity frameworks (mobile driver's licenses, EU Digital Identity Wallet).

Tier 6 — Regulatory and Compliance Infrastructure

- **AML/KYC providers** (Chainalysis, Elliptic, Jumio, Onfido);
- **Regulatory reporting systems**;
- **Qualified Custodian Infrastructure**;
- **Sanctions Screening** (OFAC, EU, UN). Hedera's native on-chain KYC/AML flags and OFAC compliance capabilities provide additional on-ledger enforcement.

Capabilities

- **Token lifecycle adapter** — maps QPT operations onto native APIs of each tier. Leverages Hedera's Asset Tokenization Studio for compliance-native issuance with ERC-1400/ERC-3643 standards, and Stablecoin Studio for fiat-pegged settlement instruments with built-in proof-of-reserve.
- **Custodian-gated fiat bridge** — routes all fiat redemption and on-ramp events through regulated custodians with AML/KYC enforcement. Connects to Tier 4 payment rails for actual value movement—card networks, real-time payments, cross-border networks, and stablecoin rails.
- **Liquidity Pool infrastructure adapter** — enables Quantum Privacy Liquidity Pools using existing AMM mechanics from Uniswap, Curve, Raydium, and Orca, with QPN governance layered on top. Real precedent: Archax Pool Tokens on Hedera providing unified liquidity for $500M+ in tokenized MMF assets.
- **Payments integration layer** — connects QPT settlement events to existing payment infrastructure. FedNow/SEPA Instant for domestic instant settlement, card networks for

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

consumer transactions, SWIFT gpi/Wise for international flows, stablecoin rails for crypto-native settlement. Supports payment initiation through open banking APIs for direct bank-to-bank settlement.

- **Individual data access and PPN activation bridge** — enables individuals to activate Personal Privacy Networks through existing consumer FinTech infrastructure. Plaid, Yodlee, and MX provide financial data access; FHIR APIs provide healthcare data; payroll APIs provide income/employment data. Each authorized stream becomes a governed QP Resource within the individual's Personal Privacy Network. No institutional permission required.
- **Securitization and structured product bridge** — enables QPT securitization into institutional-grade financial products through Securitize, tZERO, or equivalent platforms.
- **Cross-substrate token portability** — QPT instruments move across substrates (Hedera to Ethereum, on-chain to off-chain) while preserving Trust Block lineage. Leverages Hedera-Axelar (60+ chains), LayerZero, Wormhole, deBridge.
- **Price discovery and market formation** — continuous price discovery through existing exchange and AMM infrastructure. Institutional precedent: tokenized equities trading on Hedera via Swarm; tokenized MMF/gilts used as FX collateral by Lloyds Banking Group.
- **Collateralization and lending** — borrowing against QPT positions through Aave, Compound, Jupiter Lend, and TradFi securities lending with QPT-specific governance constraints.
- **Regulatory compliance orchestration** — jurisdiction-appropriate compliance pipelines with AML/KYC, sanctions screening, accredited investor verification. Leverages Hedera's native on-chain KYC/AML flags and OFAC compliance.

QPN/PNX Implementation Role

This extension provides the financial plumbing that converts the QPN/PNX from an economic settlement protocol into a fully liquid, globally accessible financial system. Without it, Exchange Tokens are settlement instruments with deferred liquidity. With it, they become tradeable, redeemable, collateralizable financial assets with continuous price discovery, institutional-grade custody, and global payment connectivity.

The Tier 5 (Consumer FinTech & Open Data Access) integration is particularly significant because it is the infrastructure through which billions of individuals can activate Personal Privacy Networks without institutional sponsorship. Plaid alone connects to 12,000+ financial institutions. FHIR APIs are legally mandated for 300M+ Americans. The infrastructure to exercise individual data rights exists at population scale—the QPN layers economic settlement, governance, and value sharing on top.

Critically, the bridge inherits operational maturity from the most heavily regulated, most rigorously tested, and most capital-intensive infrastructure in the global economy. Financial exchanges process trillions daily with 99.99%+ uptime. Payment networks process tens of billions of transactions annually. Open banking APIs connect to virtually every consumer financial account in the developed world. The QPN needs adapters, not replacements.

Incremental QPN Value Add

- **Liquidity activation for all QPT instrument classes** — converting deferred economic rights into tradeable, collateralizable financial assets through existing infrastructure.
- **Market-discovered price formation** enabling discount rates to emerge from actual transactions—supporting the market-implied discount rate mechanism.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Institutional access pathway** through familiar custody, trading, and compliance infrastructure.
- **Individual economic activation at population scale** through open banking, FHIR, and payroll APIs. Billions of individuals publish personal data as governed PNX Resources—without crypto wallets, without blockchain expertise. Existing bank accounts and health portals serve as the on-ramp.
- **Global payment connectivity** bridging PNX settlement to fiat in any currency, through any payment method, in any jurisdiction.
- **Securitization capability** for institutional-grade financial products—accessing the $130T+ global institutional investment market.
- **Tax-efficient value realization** supporting capital-asset treatment and lending against token positions without taxable disposition.
- **Multi-jurisdiction regulatory activation** through modular Tokenization Service Provider architecture.
- **Structural compression of settlement and liquidity risk** as Liquidity Pool depth increases.

Target Users

Tokenization Service Provider operators, digital asset exchange integration teams, institutional custody architects, securities structuring teams, compliance engineers, treasury management professionals, DeFi protocol developers, financial infrastructure architects, payment integration engineers, open banking platform developers, consumer FinTech application builders, healthcare IT integration teams, CBDC integration architects, and Liquidity Pool operators.

Existing Installed Base

Traditional exchanges process trillions in daily volume. DTCC clears $2 quadrillion annually. Institutional custodians safeguard $40T+. Digital asset exchanges serve tens of millions of verified accounts. Hedera has processed tens of billions of transactions with 2.9-second finality and $0.0008 average cost, hosting Archax, Swarm, StegX, Wyoming FRNT, and the Canary HBAR ETF on NASDAQ.

Visa processes 200B+ transactions annually. FedNow enables instant U.S. payments. UPI processes 10B+ monthly in India. Stripe, Adyen, and Square collectively process trillions annually.

Plaid connects to 12,000+ U.S. institutions. Yodlee connects to 17,000+ global sources. FHIR APIs cover 300M+ Americans. The combined infrastructure represents the most comprehensive financial data access layer ever built.

Total Addressable Value Enabled

This extension operates at three levels. First, aggregate QPT instrument value requiring liquidity: measured in trillions under conservative scenarios. Second, access to the $130T+ global institutional investment market. Third, population-scale Personal Privacy Network activation—reclaiming economic participation in the trillions of value currently captured by institutions from individual data.

Development Effort Estimate

Prototype / Alpha	Controlled Beta	GA

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

8–14 developer-months	**16–24 developer-months**	**28–42 developer-months**

AI Development Contribution

45–65% of development is AI-assistable. Financial API integration, token lifecycle operations on Hedera/EVM/Solana, DeFi protocol adapters, open banking API integration (Plaid, Yodlee, MX), and payment rail integration follow well-documented patterns. The primary human effort involves regulatory compliance architecture, financial security engineering, Liquidity Pool mechanism design, consumer data consent architecture, securitization structuring, and cross-substrate integrity verification. The GA timeline reflects six infrastructure tiers and rigorous security auditing requirements.

B.11.13 Quantum Privacy & Post-Quantum Cryptographic Infrastructure Bridge

Description

A cryptographic infrastructure adapter layer that enables Quantum Privacy Cells (QPCs), Quantum Privacy Domains, and the privacy-preserving computation foundations of the QPN to operate using existing and emerging post-quantum cryptography, zero-knowledge proof systems, homomorphic encryption, confidential computing, quantum entropy generation, and data sovereignty infrastructure—rather than requiring purpose-built cryptographic systems. The bridge provides the cryptographic primitives, privacy-enhancing computation substrates, and data sovereignty enforcement mechanisms through which the QPN's core privacy guarantees are implemented at infrastructure level.

Quantum Privacy Cells—the legally binding, privacy-preserving governance containers at the heart of the QPN architecture—require cryptographic enforcement that is both quantum-resistant (protecting against future quantum computing attacks, including harvest-now-decrypt-later threats) and privacy-preserving (enabling computation on encrypted or governed data without exposing it to counterparties, intermediaries, or infrastructure operators). The QPN's provisional patent filings claim systems for privacy-preserving personalization within QPCs, zero-knowledge bargaining, federated computation across Privacy Domains, and cryptographic governance enforcement—all of which depend on the cryptographic infrastructure this extension bridges to.

The extension also addresses data sovereignty and residency requirements that are essential for global QPN deployment. Quantum Privacy Domains operate within jurisdictional boundaries; governed data must remain within specified geographies while still participating in cross-border PNX settlement. Existing data sovereignty infrastructure—sovereign cloud platforms, data residency services, and cross-border data governance tools—provides the operational substrate for jurisdictionally compliant QPC operation.

Critically, the "quantum" in Quantum Privacy is not merely aspirational—it refers to the architectural requirement that QPN privacy guarantees remain sound even against quantum computing adversaries. This extension ensures that the cryptographic foundations of every QPC, every Trust Block signature, every settlement proof, and every governance attestation in the PNX are quantum-resistant from initial deployment, not retrofitted after quantum threats materialize.

Target Platforms

Tier 1 — Post-Quantum Cryptography (PQC) & Quantum Entropy

- **Quantropi QiSpace platform**: MASQ asymmetric encryption (smallest public key and signature sizes of any PQC candidate, fastest sign and verify), QEEP symmetric encryption

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

(quantum-secure, up to 18x faster than AES-256), SEQUR quantum entropy services including synchronized digital quantum key distribution (QKD) over existing networks.

- **Quside quantum random number generators (QRNGs):** hardware-based Level 4 verifiable quantum entropy using VCSEL laser phase fluctuations; Garnet Series PCIe QRNGs (100 Mbit/s to 1 Gbit/s); mass-manufacturable quantum entropy source demonstrated with Coherent Corp at Photonics West 2026; NIST SP800-90B certified; deployed in QKD systems, financial Monte Carlo acceleration, and satellite-based key distribution. NIST PQC standards: ML-KEM (Kyber) for key encapsulation, ML-DSA (Dilithium) for digital signatures, SLH-DSA (SPHINCS+) for stateless hash-based signatures.
- **Additional PQC implementations**: Open Quantum Safe (liboqs), PQShield, ISARA, IBM post-quantum toolkit.

Tier 2 — Zero-Knowledge Proof Systems

- **zk-SNARK implementations** (Groth16, PLONK, Halo2) for succinct non-interactive proofs enabling Trust Block verification, governance attestation, and settlement proof without revealing underlying data. zk-STARK implementations for transparent, post-quantum-resistant zero-knowledge proofs without trusted setup—critical for QPN's trust-minimized architecture.
- **Midnight** (Cardano's zero-knowledge privacy layer, targeting full decentralized mainnet Q3 2026) for privacy-preserving smart contracts.
- **Aztec Network** for private computation on Ethereum.
- **Mina Protocol** for constant-size blockchain proofs. Circom, Noir, and Leo for zero-knowledge circuit development and compilation.
- **ZK rollup infrastructure** (zkSync, StarkNet, Polygon zkEVM) for scalable, privacy-preserving settlement computation.

Tier 3 — Homomorphic Encryption & Secure Multiparty Computation

- **Fully homomorphic encryption** (FHE): Microsoft SEAL, Zama (TFHE-rs and Concrete), HElib (IBM), OpenFHE—enabling computation on encrypted QPC-governed data without decryption.
- **Secure multiparty computation** (MPC): Sharemind, SCALE-MAMBA, MP-SPDZ—enabling multiple parties to jointly compute settlement, pricing, or governance functions without revealing individual inputs.
- **Functional encryption libraries** for selective attribute disclosure within QPCs.
- **Differential privacy frameworks** (Google DP library, OpenDP, Apple's local differential privacy) for statistical disclosure control in aggregated PNX analytics.

Tier 4 — Confidential Computing & Hardware-Based Trust

- **Intel SGX and TDX** (Trust Domain Extensions) for hardware-isolated trusted execution environments.
- **AMD SEV-SNP** (Secure Encrypted Virtualization with Secure Nested Paging) for VM-level confidential computing.
- **ARM Confidential Compute Architecture** (CCA) for mobile and edge confidential processing.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **NVIDIA H100/H200 Confidential Computing** for GPU-accelerated privacy-preserving AI inference within QPCs.
- **Confidential computing cloud services**: Azure Confidential Computing, AWS Nitro Enclaves, Google Confidential VMs.
- **Hardware Security Modules (HSMs)**: Thales Luna, Entrust nShield, AWS CloudHSM, Azure Dedicated HSM for cryptographic key management and signing operations.
- **Enterprise PKI infrastructure**: DigiCert, Sectigo, Let's Encrypt for certificate lifecycle management;
- **HashiCorp Vault** and **CyberArk Conjur** for secrets management and cryptographic key orchestration.

Tier 5 — Data Sovereignty, Residency & Cross-Border Governance

- **InCountry**: Data Residency-as-a-Service (DRaaS) and Data Sovereignty-as-a-Service enabling in-country data storage and processing across 90+ countries; AgentCloak for AI agent data protection with sovereign AI models trained on local languages and regulatory requirements; digital twin technology for data cloaking and cross-border compliance;
- **MCP Server/Proxy** integration for agentic workflows; supports GDPR, PIPL (China), PDPL (Saudi Arabia), EU AI Act, and jurisdiction-specific data localization mandates.
- **Microsoft Sovereign Cloud** (sovereign public cloud with in-country data processing for M365 Copilot in 15+ countries, Sovereign Private Cloud via Azure Local for air-gapped deployments).
- **AWS European Sovereign Cloud** (€7.8B investment, fully isolated EU infrastructure). Google Distributed Cloud (Secret/Top Secret authorization, on-premises sovereign deployment).
- **BigID** for AI-driven data discovery and classification supporting residency enforcement. Skyflow for geography-specific privacy vaults and tokenized data storage. Data sovereignty compliance market: $72B in 2025, projected $228B by 2030 at 25.8% CAGR.

Tier 6 — Privacy-Preserving Machine Learning & Federated Computation

- **Federated learning frameworks**: Google TensorFlow Federated, NVIDIA FLARE, PySyft (OpenMined), Flower—enabling AI model training across distributed QPCs without centralizing data.
- **Privacy-preserving inference**: NVIDIA Confidential Computing for GPU-based AI inference within trusted execution environments.
- **Synthetic data generation**: Gretel.ai, MOSTLY AI, Hazy—for producing privacy-safe training data that preserves statistical properties without exposing individual records.
- **De-identification and anonymization tools**: ARX Data Anonymization Tool, Privitar, Anonos—for HIPAA Safe Harbor and Expert Determination de-identification within healthcare QPCs.

Capabilities

- **Quantum-resistant QPC cryptographic envelope** — implements the cryptographic boundary of every Quantum Privacy Cell using post-quantum key encapsulation (ML-KEM/Kyber), post-quantum digital signatures (ML-DSA/Dilithium), and quantum-generated entropy (Quside QRNGs, Quantropi SEQUR) for key material. Every QPC's governance boundary, consent record, and Trust Block signature is quantum-resistant

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

from deployment. Supports crypto-agility through Quantropi's QiSpace platform, enabling seamless algorithm rotation as PQC standards evolve.

- **Zero-knowledge governance verification** — enables Trust Block validation, Proof of Trust attestation, and settlement proof verification without revealing the underlying governed data, policies, or participant attributes. A counterparty can verify that a QPC's governance satisfies specific Trust Criteria without seeing the data, the policies, or the identity of the QPC holder. Implements the zero-knowledge bargaining and privacy-preserving governance verification claimed in the QPN's provisional patents.
- **Encrypted computation within Privacy Domains** — enables the Personalized Exchange Engine (B.11), AI Content Engine (B.16), and other settlement-generating operations to compute on QPC-governed data without decryption through homomorphic encryption, secure multiparty computation, or confidential computing enclaves. Personalization occurs on authorized attributes within the Privacy Domain; the computation infrastructure never sees plaintext.
- **Hardware-rooted trust for settlement infrastructure** — anchors critical QPN operations (Trust Block signing, Exchange Token issuance, Liquidity Pool settlement, EasyAccess credential generation) in hardware-based trusted execution environments and HSMs. Provides tamper-evident, attestable compute environments that counterparties and auditors can verify independently.
- **Jurisdictional data sovereignty enforcement** — ensures Quantum Privacy Domains operate within required geographic boundaries using InCountry's DRaaS, sovereign cloud infrastructure, and data residency enforcement. QPC-governed data remains within specified jurisdictions while settlement metadata (cryptographic proofs, Exchange Token allocations, governance attestations) can flow cross-border without exposing governed data. Supports the QPN's global deployment model where QPCs operate under local jurisdiction while participating in cross-border Exchange Networks.
- **Privacy-preserving AI model operations** — enables AI models to train on, infer from, and generate content using QPC-governed data without the model operator accessing the data in plaintext. Combines federated learning (model goes to data, not data to model), confidential computing (computation in hardware-isolated enclaves), and differential privacy (statistical guarantees on output disclosure) to implement the QPN's privacy-preserving AI architecture.
- **Crypto-agile infrastructure adaptation** — provides abstraction layers that allow the QPN's cryptographic primitives to be upgraded without disrupting deployed QPCs, Trust Blocks, or settlement records. As PQC standards mature, as new zero-knowledge proof systems emerge, and as quantum computing threats evolve, the bridge enables algorithm rotation across the entire PNX without requiring re-issuance of existing cryptographic commitments.
- **Cross-border privacy-preserving settlement** — enables Exchange Token settlement across jurisdictional boundaries without violating data sovereignty requirements. Settlement proofs (zero-knowledge), governance attestations (encrypted), and token allocation records (deterministic computation outputs) cross borders; governed data does not. InCountry's digital twin and data cloaking technology provides the operational mechanism for maintaining global settlement visibility while enforcing local data residency.

QPN/PNX Implementation Role

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

This extension provides the cryptographic and privacy infrastructure layer upon which every other QPN component depends. Quantum Privacy Cells cannot exist without quantum-resistant cryptographic envelopes. Trust Blocks cannot be signed without post-quantum digital signatures. Zero-knowledge governance verification cannot operate without ZK proof systems. Privacy-preserving personalization cannot function without encrypted computation capabilities. Cross-border settlement cannot comply with data sovereignty laws without residency enforcement infrastructure.

The extension is architecturally foundational: it sits beneath the resource publishing extensions (B.1–B.10), the economic decisioning layer (B.11), the financial infrastructure (B.12), the identity layer (B.14), the governance layer (B.15), and the content generation layer (B.16). Every cryptographic operation in the PNX—from QPC creation to Trust Block signing to Exchange Token issuance to settlement proof generation—routes through the primitives this extension bridges to.

The vendor landscape is critical. Quantropi provides the only platform offering all three prerequisites for end-to-end quantum security: post-quantum asymmetric encryption, quantum-secure symmetric encryption, and quantum entropy services—deployable over existing networks. Quside provides hardware-based verifiable quantum entropy at the silicon level, enabling quantum-grade randomness to be embedded in processors, secure elements, and hardware roots of trust at mass-manufacturing scale. InCountry provides the data sovereignty enforcement that enables QPCs to operate within jurisdictional boundaries while participating in global Exchange Networks. Together with enterprise HSM, PKI, confidential computing, and ZK proof infrastructure, these form the complete cryptographic substrate for QPN deployment.

The provisional patents' claims on privacy-preserving computation within QPCs, zero-knowledge governance verification, and cryptographic settlement proof are all implemented through the infrastructure this extension bridges to. Without this extension, the QPN's privacy guarantees are architectural aspirations; with it, they are cryptographically enforced at infrastructure level.

Incremental QPN Value Add

- **Quantum-resistant privacy guarantees from day one** — every QPC, Trust Block, and settlement record is protected against both classical and quantum adversaries, including harvest-now-decrypt-later attacks on long-duration PNX value streams that may persist for decades.
- **Cryptographic enforcement of privacy promises** — the QPN's privacy architecture is not policy-dependent (where violations are detected after the fact) but cryptographically enforced (where violations are computationally infeasible). This is the structural distinction between QPN privacy and conventional privacy compliance.
- **Zero-knowledge governance enabling frictionless cross-organizational settlement** — counterparties verify governance compliance without seeing each other's data, policies, or internal systems. This eliminates the bilateral compliance review overhead that currently prevents most cross-organizational data collaboration.
- **Jurisdictional compliance at infrastructure level** — data sovereignty enforcement through InCountry, sovereign cloud, and residency infrastructure means QPN operators can deploy globally without jurisdiction-by-jurisdiction legal review of data flow patterns. Compliance is embedded in infrastructure, not bolted on through legal agreements.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Privacy-preserving AI as a competitive differentiator** — enables AI models to generate personalized value from QPC-governed data without accessing plaintext, creating a privacy-preserving AI capability that surveillance-based competitors cannot match.
- **Hardware-rooted trust reducing counterparty risk** — settlement operations anchored in HSMs and confidential computing enclaves provide cryptographic assurance that cannot be repudiated, reducing the trust assumptions required between PNX participants.
- **Crypto-agility ensuring long-term infrastructure viability** — the QPN's cryptographic foundations can evolve with the threat landscape without disrupting deployed economic relationships, protecting the multi-decade value streams that PNX settlement generates.
- **Data sovereignty market alignment** — positions the QPN within the $72B (growing to $228B by 2030) data sovereignty compliance market, where every enterprise deploying QPCs becomes a customer of the sovereignty infrastructure this extension bridges to.

Target Users

Chief information security officers (CISOs), cryptographic engineers, privacy engineers, security architects, confidential computing specialists, post-quantum migration teams, data protection officers (DPOs), sovereignty compliance teams, HSM and PKI administrators, zero-knowledge proof developers, federated learning engineers, and QPC infrastructure operators.

Existing Installed Base

The post-quantum cryptography migration is already underway across the global technology ecosystem. NIST finalized PQC standards in 2024; major cloud providers (AWS, Azure, Google Cloud) have begun integrating PQC into their services. Quantropi's QiSpace platform is commercially available with NIST-aligned PQC and quantum entropy services. Quside's QRNGs are deployed in production QKD systems, financial services, and satellite-based key distribution, with mass-manufacturable silicon-level quantum entropy demonstrated with Coherent Corp. The confidential computing installed base spans hundreds of millions of Intel SGX/TDX-capable processors, AMD SEV-SNP-enabled servers, and ARM CCA-capable mobile devices. HSMs from Thales and Entrust protect critical infrastructure across banking, government, and healthcare globally.

The zero-knowledge proof ecosystem has matured rapidly. Ethereum L2s (zkSync, StarkNet, Polygon zkEVM) process billions in transaction volume using ZK proofs. Midnight targets production privacy-preserving smart contracts in 2026. The ZK toolchain (Circom, Noir, Halo2) supports production deployment of custom proof circuits.

InCountry provides data residency services in 90+ countries, serving Global 2000 companies in life sciences, semiconductors, and financial services. The sovereign cloud market exceeds $154B in 2025 and is projected to reach $823B by 2032. Microsoft, AWS, and Google have each made multi-billion-dollar sovereign cloud investments. Every enterprise operating under GDPR, PIPL, PDPL, or other data localization mandates is a potential consumer of the sovereignty infrastructure this extension bridges to.

Total Addressable Value Enabled

This extension's addressable value operates at three levels. First, the post-quantum cybersecurity market: global cybersecurity spending exceeds $200B annually, and every cryptographic system in the world must eventually migrate to PQC—the QPN provides both a forcing function and an economic model for this migration. Second, the data sovereignty compliance market ($72B in 2025, $228B by 2030) represents the direct cost of jurisdictional data governance that this extension transforms from overhead into PNX-integrated infrastructure. Third, and most consequentially, this extension enables the multi-trillion-dollar

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

cross-organizational data collaboration market that is currently blocked by privacy and sovereignty barriers: healthcare data networks ($3–5T addressable), financial data sharing ($5–10T), cross-border government data cooperation, and industrial data ecosystems. The QPN's cryptographic privacy infrastructure converts these barriers from blockers into enablers by making privacy-preserving cross-organizational settlement computationally feasible at global scale.

Development Effort Estimate

Prototype / Alpha	Controlled Beta	GA
8–12 developer-months	**14–20 developer-months**	**24–36 developer-months**

AI Development Contribution

40–60% of development is AI-assistable. API integration with PQC libraries (liboqs, Quantropi SDKs), confidential computing SDKs (Intel SGX SDK, AMD SEV SDK), and data sovereignty platforms (InCountry REST APIs) follows well-documented patterns amenable to AI code generation. ZK circuit development using Circom and Noir is increasingly AI-assistable with established patterns. HSM integration and PKI configuration follow standardized PKCS#11 and KMIP interfaces.

The primary human effort involves cryptographic protocol design (ensuring QPC envelope construction, Trust Block signing, and settlement proof generation are provably secure under post-quantum threat models), ZK circuit optimization (achieving acceptable proof generation and verification performance for real-time settlement operations), confidential computing attestation architecture (designing remote attestation flows that counterparties can verify independently), and data sovereignty compliance mapping (translating jurisdiction-specific data localization requirements into machine-enforceable QPC boundary rules). Formal verification of cryptographic constructions is essential and requires specialized expertise. The GA timeline reflects the breadth of cryptographic, sovereignty, and confidential computing tiers, the criticality of security correctness, and the need for independent security auditing of every cryptographic component.

B.11.14 Identity Resolution, Verification & Trust Attestation Layer

Description

An identity intelligence, entity resolution, and trust verification adapter layer that enables the EasyAccess Authorization Network, Proof of Trust verification, and the Unified Trust Model (UTM) to operate using the existing global installed base of identity resolution, entity resolution, data tokenization, identity verification, authentication, biometric, fraud detection, decentralized identity, and governance risk and compliance (GRC) infrastructure—rather than requiring purpose-built identity and trust systems. The bridge provides the identity resolution, verification, authentication, and trust attestation primitives through which the QPN's core identity and governance constructs are implemented at operational scale.

Critically, this extension is designed around a multi-vendor aggregation and dual-use deployment model. The global identity resolution, tokenization, and verification ecosystem is already fragmented across dozens of competing vendors, each maintaining proprietary identifier graphs, resolution algorithms, and customer deployments. Enterprises have already paid these vendors to resolve, verify, and enrich their data. The QPN does not seek to replace this existing spend—it seeks to aggregate and reuse it. Each vendor's outputs (resolved identities, persistent identifiers, tokenized records, verified attributes) can be ingested, cryptographically tokenized, and linked into a global privacy graph at near-zero marginal cost,

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

because the resolution work has already been performed and paid for by the vendor's existing customers.

This creates a powerful dual-use value proposition for identity vendors. In the current model, identity resolution vendors sell their services once to enterprises for internal data management. Under the QPN model, vendors can offer native EasyAccess Authorization Network implementations and Privacy Domain integrations to their existing customers at no additional cost to the enterprise, funded instead by a revenue share on the Exchange Token settlement that the vendor's identity resolution enables. The vendor's existing resolution outputs become inputs to a global privacy-preserving identity graph; the vendor receives ongoing revenue from every PNX transaction that traverses identities they resolved; and the enterprise customer receives QPN participation and Exchange Token compensation for data assets they were already maintaining. Every vendor implementation expands the graph, making the network more valuable for all other participants—a self-reinforcing adoption dynamic.

The EasyAccess Authorization Network operates as a dual-use overlay on existing identity and access management (IAM) systems. It does not replace enterprise identity providers; it layers QPC-mediated consent, privacy-preserving credential management, and cross-organizational identity interoperability on top of them. Proof of Trust—the QPN's mechanism for verifying that participants, resources, and governance frameworks satisfy specified Trust Criteria within the Unified Trust Model—requires continuous identity verification, entity resolution across data sources, behavioral and device intelligence, and compliance attestation. The Unified Trust Model (UTM) defines the taxonomy and interoperability framework through which Trust Criteria authored in one domain can be mapped to Trust Criteria in another domain.

Target Platforms

Tier 1 — Credit Bureau & Consumer Identity Resolution Graphs

The three major credit bureaus operate the largest consumer identity graphs in the world, each maintaining persistent identifiers for virtually every adult in the United States and increasingly globally. These graphs represent decades of continuous identity resolution investment and are the foundational layer upon which most enterprise identity operations already depend.

- **Experian**: AI-driven identity resolution unifying offline and online data across Digital Graph and Offline Graph; resolves billions of digital identifiers (MAIDs, CTV IDs, universal IDs, hashed emails) to individuals and households; ranked #1 in accuracy by Truthset; GLBA/FCRA-compliant, GDPR/CCPA-ready; supports cookieless identifiers including UID2, ID5, and Hadron ID; Graph rebuilt weekly for accuracy; 30+ direct and 200+ indirect activation destination partnerships; revenue-share structures for third-party data onboarding; Experian Marketing Services serves as data collaboration and enrichment platform.
- **LexisNexis Risk Solutions** LexID: Proprietary persistent identifier resolving, matching, and managing over 283 million U.S. consumer identities with 99%+ confidence; built from 83 billion+ public records and 10,000+ data sources; refreshed with 80 million+ new records per month; non-SSN-dependent identifier providing safer alternative to traditional PII; Scalable Automated Linking Technology (SALT) patented method for linking and clustering data; LexID Digital extends to the digital realm by unifying LexID with ThreatMetrix Digital Identity Network's 1.4B+ tokenized digital identities and 35 billion+ annual crowdsourced global transactions, creating 360-degree offline-to-online identity view; deployed across insurance (underwriting, claims, cross-sell), financial services (KYC, fraud), healthcare, and government.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **TransUnion TruAudience** (incorporating Neustar OneID): Enhanced identity graph integrating TransUnion's offline consumer data (125 million+ U.S. households) with Neustar's OneID identity resolution platform; 200 authoritative data sources spanning 16 billion monthly phone signals and 10 billion real-time digital interactions daily; AI-driven four-stage process (data sourcing, matching, linking clusters, scoring identities) clustering identifiers into individuals and households; OneTru platform unifying identity across credit risk (TruVision), fraud (TruValidate), and marketing (TruAudience); Snowflake Native App for cloud-based identity resolution; operational in U.S. and India with planned expansion to Canada, Philippines, and U.K.; 13,000+ associates operating in 30+ countries.

Tier 2 — Advertising, Marketing & Data Collaboration Identity Graphs

- **LiveRamp**: Leading data collaboration platform with RampID, the industry's most interoperable persistent pseudonymous identifier; AbiliTec offline recognition technology resolving separate emails, postal addresses, and phone numbers to individuals using patented algorithms against multi-billion-record reference bases; largest deterministic identity graph with PII maintained on 245 million+ U.S. individuals; resolves MAIDs, CTV IDs, cookies, hashed emails, phone numbers, and custom IDs; integrated with AWS Entity Resolution and Snowflake; authenticated traffic solution deployed across 92% of the advertising ecosystem including Disney, Netflix, Spotify, TikTok, and Roku; 900+ global customers including many Fortune 500; Safe Haven clean room for privacy-preserving data collaboration; Local Encoder enabling RampID generation within customer's own cloud environment.
- **The Trade Desk Unified ID 2.0** (UID2) and European Unified ID (EUID): Open-source identity framework converting authenticated email and phone data into hashed, salted, encrypted pseudonymous identifiers; adopted by major ad tech platforms, SSPs, and DSPs globally; consumer opt-out portal providing universal transparency and control; IAB Tech Lab governance; interoperable with other identity solutions; decentralized storage (no centralized PII); Roku, Perion, Criteo, and hundreds of publishers integrated; EUID launched for European market on Snowflake Marketplace with GDPR-compatible design; the dominant open identity standard for the post-cookie advertising ecosystem.

Tier 3 — Healthcare Identity Resolution, Tokenization & Privacy-Preserving Record Linkage

- **Datavant**: Healthcare data collaboration platform processing 60 million+ records across thousands of organizations; patented tokenization technology replacing sensitive patient information with encrypted tokens that cannot be reverse-engineered; ubiquitous token enabling cross-dataset patient matching without sharing underlying PII; tokens generated on-premises behind customer firewalls (Datavant never accesses patient data); privacy-preserving record linkage (PPRL) deployed in 270+ clinical trials; referential data integration for high-confidence matching across records with different PII; partners with Databricks clean rooms and AWS Clean Rooms; 75% of the 100 largest U.S. health systems; 350+ real-world data partners; 80,000+ hospitals and clinics; advocating for federal PET (privacy-enhancing technology) standards; market leader in HIPAA-compliant health data linkage.
- **HealthVerity**: Leader in Identity, Privacy, Governance, and Exchange (IPGE) for real-world healthcare data; HealthVerity ID (HVID) universal identifier generated through three-step privacy architecture (behind-firewall PII hashing, independent matching environment, client-specific HVID generation—HealthVerity never sees PII or encrypted hashes); probabilistic identity resolution achieving 10x improvement over legacy tokenization accuracy; processing 1 million+ HVIDs per minute in real-time; 150 billion+ de-identified transactions across 330 million+ American patients from 75+ data sources in HealthVerity

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Marketplace; HIPAA compliance certified by Dr. Brad Malin of Vanderbilt University; FedRAMP authorized at Moderate security level with 40+ federal agency ATOs; patented privacy computing environment enabling SDOH analysis without violating HIPAA; Verified Data framework ensuring source traceability and eliminating synthetic data creep.

- **Symphony Health Synoma (ICON plc):** Proprietary Synoma® tokenization engine de-identifying and integrating healthcare data via unique patient tokens; 10 billion+ patient transactions processed annually; 95%+ match rates validated by independent third parties; Integrated Dataverse (IDV) linking prescriptions, medical claims, hospital data, EHRs, and lab results for 305 million+ U.S. patients across 900,000+ data sources (3+ petabytes); interoperable with Datavant token ecosystem; clinical trial tokenization enabling real-world evidence linkage for pre- and post-marketing authorization; won 2024 Silver Stevie Award for Healthcare Technical Innovation; supports HEOR, market access, commercial analytics, and regulatory submissions.

Tier 4 — Entity Resolution & AI-Powered Identity Intelligence

- **Senzing**: Real-time AI-powered entity resolution SDK with <200ms resolution latency; Entity Centric Learning for self-tuning, self-correcting, sequence-neutral identity matching; sixth-generation system refined over 40+ years; handles messy, incomplete, and intentionally obfuscated data; explainable results with Match Key Details, Record Preview API, and Feature Traceability (v4, October 2025); relationship discovery (households, networks, fraud rings); deployed on-premises or cloud with no data flowing to Senzing; available on Microsoft Azure Marketplace (November 2025); 30+ years and $50M+ development investment by founder Jeff Jonas.
- **Additional entity resolution platforms**: These platforms collectively represent the enterprise MDM and entity resolution infrastructure that can be adapted to resolve identities within QPCs and across Exchange Networks:
  - **IBM InfoSphere** Master Data Management,
  - **Informatica MDM**,
  - **Reltio Connected Data Platform** (cloud-native connected data),
  - **Tamr** (AI-driven data mastering),
  - **Amperity** (customer data platform with AI identity resolution used by major retailers and consumer brands).
  - **AWS Entity Resolution** (native AWS service with LiveRamp, TransUnion, and other provider integrations).

Tier 5 — Identity Verification & Document Authentication

LexisNexis Risk Solutions: **ThreatMetrix** platform powering the Digital Identity Network (1.4B+ tokenized digital identities, 110M+ daily authentication decisions); **IDVerse** for AI-driven document authentication (16,000+ global identity documents, 99.98% biometric face-matching accuracy, deepfake detection); Behavioral Biometrics for continuous passive authentication. **Jumio**: AI-driven identity verification with document scanning, biometric verification, and liveness detection. **Onfido**: automated identity verification across 195 countries. **Veriff**: video-based identity verification with AI-assisted fraud detection. **Socure**: identity verification and fraud prediction from 19,000+ digital sources. **ID.me**: identity verification for government services with 130M+ verified identities. Identity verification market: $14.3B in 2025, projected $29.3B by 2030 at 15.4% CAGR.

Tier 6 — Authentication & Access Management (EasyAccess Overlay Targets)

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Enterprise IAM platforms that EasyAccess overlays as a dual-use authorization layer: **Okta** (18,000+ enterprise customers, Universal Directory, Adaptive MFA, CIAM), **Microsoft Entra ID** (formerly Azure AD, 600M+ users, conditional access, workload identities), **Ping Identity** (enterprise federation and API security, now merged with ForgeRock), **SailPoint** (identity governance and administration, access certification), **CyberArk** (privileged access management, identity security). **FIDO2/WebAuthn** passkey infrastructure: 15B+ user accounts enabled globally (Apple Passkeys, Google Passkeys, Windows Hello, YubiKey hardware keys). **OAuth 2.0, OIDC**, and **SAML** federation deployed across virtually every enterprise web application globally.

Tier 7 — Behavioral Biometrics & Continuous Authentication

BioCatch: behavioral biometric intelligence for financial services, detecting account takeover, social engineering, and money mule activity through cognitive and physiological behavioral analysis; 32B+ annual sessions analyzed; deployed by major banks globally. LexisNexis Behavioral Biometrics (integrated within ThreatMetrix). **TypingDNA**: typing biometrics for continuous user verification. **Plurilock**: continuous endpoint authentication. **Device intelligence**: LexisNexis Digital Identity Network device profiling, Sardine (device and behavior intelligence for fintech), Castle (real-time threat detection).

Tier 8 — Decentralized Identity & Verifiable Credentials

W3C Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) standards. Hedera DID method and Verifiable Credential infrastructure. Microsoft ION (DID network built on Bitcoin). Hyperledger Indy/Aries for privacy-preserving credential exchange with selective disclosure. EU Digital Identity Wallet (EUDI Wallet) mandated by eIDAS 2.0 for all EU member states by 2026. Mobile driver's license (mDL) infrastructure under ISO 18013-5, deployed or piloting in 30+ U.S. states. cheqd for credential payment and verification infrastructure. Spruce ID and SpruceKit for developer tooling.

Tier 9 — GRC, Trust Framework & Compliance Attestation Platforms

CENTRL: GRC automation for third-party risk management, vendor assessments, and compliance orchestration. **ServiceNow GRC** (integrated risk management within the ServiceNow platform). **OneTrust** (privacy management, GRC, consent management across 100+ regulatory frameworks). **Vanta** and **Drata** (automated security compliance for SOC 2, ISO 27001, HIPAA, PCI DSS). LogicGate Risk Cloud, Archer (RSA), TrustArc. Regulatory intelligence: Thomson Reuters Regulatory Intelligence, Wolters Kluwer, LexisNexis for tracking regulatory changes affecting Trust Criteria specifications.

Tier 10 — Fraud Detection, Risk Intelligence & Sanctions Screening

LexisNexis Digital Identity Network: cross-industry fraud intelligence from billions of monthly contributed transactions. TransUnion **TruValidate**: fraud prevention and identity proofing powered by OneTru platform with improved fraud capture rates. **Chainalysis** and **Elliptic** for blockchain transaction monitoring and cryptocurrency compliance. **Dow Jones Risk & Compliance** and **Refinitiv World-Check** for sanctions screening, PEP identification, and adverse media monitoring. **Featurespace**, **Sardine**, **ComplyAdvantage**, **NICE Actimize** for financial crime detection and risk management.

Capabilities

- **Multi-vendor identity graph aggregation and cross-linkage** — ingests resolved identity outputs from all Tier 1–4 vendors (Experian identity graphs, LexisNexis LexID/LexID Digital, TransUnion/Neustar OneID identity graph, LiveRamp RampID/AbiliTec, Datavant tokens, HealthVerity HVIDs, Symphony Health Synoma tokens, Senzing entity resolution outputs,

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

and UID2/EUID identifiers) and cryptographically links them within Privacy Domains to create a global privacy-preserving identity graph. Each vendor's resolution outputs are tokenized using the cryptographic infrastructure provided by B.13 and linked through privacy-preserving record linkage (PPRL) techniques without requiring any vendor to share their proprietary graph data with any other vendor. The resulting meta-graph enables QPC identity anchoring that inherits the accuracy and coverage of all contributing vendors simultaneously—a capability no single vendor can achieve alone.

- **Dual-use vendor deployment with revenue-share economics** — enables identity resolution, tokenization, and verification vendors to deploy native EasyAccess Authorization Network connectors and Privacy Domain integrations as extensions to their existing enterprise products. Vendors offer these capabilities to existing customers at no additional cost (or as value-added premium services), funded by a revenue share on Exchange Token settlement that flows through identities they resolved. The vendor's existing enterprise deployment becomes a dual-use QPN integration point; the vendor receives ongoing PNX settlement revenue proportional to the volume of transactions traversing their resolved identities; and the enterprise customer receives QPN participation without incremental identity infrastructure spend. This creates a vendor adoption flywheel: each new vendor integration expands the global graph, increasing settlement volume and revenue-share payments, incentivizing additional vendor adoption.
- **Zero-marginal-cost identity aggregation from existing enterprise spend** — enterprises have already paid their identity vendors (Experian, LexisNexis, TransUnion, LiveRamp, Datavant, HealthVerity, etc.) to resolve, verify, and enrich their data. The QPN aggregates these already-performed resolution outputs into the global privacy graph at near-zero incremental cost to the enterprise, because the resolution work has already been completed. The enterprise's existing data management rights (which include the right to use resolved identities for their own business operations) are extended through EasyAccess consent to participate in QPN Exchange Networks. No new data processing is required—only the cryptographic tokenization and cross-linkage of existing resolution outputs.
- **EasyAccess credential bridge with universal IAM overlay** — enables the EasyAccess Authorization Network to integrate with existing IAM platforms (Okta, Microsoft Entra ID, Ping Identity, ForgeRock, SailPoint) as a dual-use overlay. EasyAccess credentials are mapped to and from existing enterprise identity attributes through standard federation protocols (OAuth 2.0, OIDC, SAML) and decentralized identity standards (W3C DIDs, Verifiable Credentials). Existing enterprise logins become EasyAccess-compatible without requiring users to adopt new credentials.
- **Cross-domain identity resolution spanning healthcare, financial services, marketing, and government** — links domain-specific identity resolution (Datavant/HealthVerity/Synoma in healthcare, LexID/Experian in financial services, RampID/UID2 in advertising, ID.me in government) into a unified privacy-preserving graph that enables cross-domain Exchange Networks. A patient identified through HealthVerity's HVID can participate in healthcare QPCs that settle against consumer attributes resolved through Experian's identity graph, all without either vendor or domain seeing the other's data. This cross-domain linkage is the structural innovation that makes the QPN's multi-industry Exchange Networks possible.
- **Real-time entity resolution for QPC identity anchoring** — uses Senzing's real-time entity resolution (<200ms) with self-correcting Entity Centric Learning to continuously resolve, link, and disambiguate identities across data sources feeding QPC identity anchors. Detects synthetic identities, resolves name/address/attribute variations across languages

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

and jurisdictions, and discovers non-obvious relationships that inform Trust Block governance and risk assessment.

- **Proof of Trust attestation engine with multi-vendor evidence aggregation** — generates machine-verifiable Proof of Trust attestations by aggregating evidence from identity verification (all Tier 5 vendors), entity resolution (Tiers 1–4), behavioral monitoring (Tier 7), compliance checks (Tier 9), and fraud/sanctions screening (Tier 10) into signed attestation packages. Integrates with GRC platforms (CENTRL, ServiceNow GRC, OneTrust, Vanta) for continuous compliance monitoring. Proof of Trust attestations are cryptographically signed using B.13's post-quantum infrastructure.
- **Unified Trust Model interoperability engine** — enables Trust Criteria authoring, semantic mapping, and cross-domain interoperability through GRC and regulatory intelligence infrastructure. Generates semantic mappings between Trust Criteria from different domains (HIPAA ↔ GDPR ↔ PIPL ↔ SOC 2 ↔ ISO 27001), enabling Resources governed under one framework to satisfy Trust Block requirements defined under another. Regulatory intelligence feeds automatically flag Trust Criteria requiring updates when regulations change.
- **Healthcare-specific privacy-preserving identity linkage** — implements HIPAA-compliant identity resolution using Datavant's ubiquitous token, HealthVerity's HVID, and Symphony Health's Synoma tokens for patient-level data linkage across claims, EHR, lab, pharmacy, and clinical trial datasets. Supports both Safe Harbor and Expert Determination de-identification methods. Enables the healthcare Exchange Networks described in the QPN's provisional patent filings—privacy-preserving personalization within healthcare QPCs that link patient data across providers, payers, and life sciences organizations without exposing PHI.
- **Continuous risk monitoring and adaptive trust scoring** — maintains real-time trust scores by continuously ingesting signals from identity verification, behavioral biometrics, entity resolution, fraud detection, and sanctions screening. Trust scores inform dynamic Trust Block governance and integrate with the Personalized Exchange Engine (B.11) to factor trust into pricing and offer routing.
- **Decentralized credential exchange and population-scale issuance** — enables EasyAccess credentials, Proof of Trust attestations, and governance certifications to be expressed as W3C Verifiable Credentials with selective disclosure via ZK-proof presentations. EU Digital Identity Wallet (mandated 2026) and mobile driver's license infrastructure provide population-scale issuance channels for EasyAccess-compatible verifiable credentials.

QPN/PNX Implementation Role

This extension is the identity and trust intelligence layer of the QPN—and, through the multi-vendor aggregation model, it is the mechanism by which the QPN inherits the identity-resolution infrastructure the global economy has already built and paid for.

The strategic insight is that identity resolution is not a single-vendor capability—it is a distributed, multi-vendor ecosystem where each vendor has resolved a partial view of the world's identities using their proprietary algorithms, data sources, and customer relationships. No single vendor has a complete view. The QPN does not need to build a complete view; it needs a privacy-preserving aggregation layer that can cryptographically link the partial views from all vendors into a unified graph without any vendor seeing any other vendor's data. This is exactly what the combination of B.13's cryptographic infrastructure and B.14's multi-vendor adapter layer provides.

The economics are transformative. Enterprises collectively spend tens of billions annually on identity resolution, verification, enrichment, and management across the vendors enumerated

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

in this extension. All of this spend produces resolved identity outputs that currently serve only the purchasing enterprise's internal operations. The QPN's dual-use model transforms each of these existing outputs into a node in a global privacy graph—at zero incremental resolution cost—while generating new Exchange Token revenue that is shared among the enterprise, the vendor, and the QPN infrastructure. The vendor's existing $X of annual enterprise revenue is not cannibalized; it is supplemented by a new revenue stream from PNX settlement that the vendor could not access without QPN integration.

The adoption flywheel operates as follows: **(1)** the Vendor, integrator, customer, or grassroots developer implements EasyAccess connector and Privacy Domain integration. **(2)** Vendor's existing enterprise customers opt in to QPN participation through EasyAccess consent. **(3)** The vendor's resolved identities are cryptographically linked into the global privacy graph. (4) Exchange Token settlement flows through those identities, generating revenue share for the vendor. (5) EasyAccess connector stakeholders promote QPN integration to more customers to increase settlement volume and revenue share. (6) More identities in the graph increase match rates and settlement opportunities for all participants, attracting more vendors. This flywheel can bootstrap from any single vendor integration and becomes self-sustaining once settlement volume generates meaningful revenue share.

The provisional patents' claims on EasyAccess dual-use authorization, QPC-mediated identity governance, Trust Criteria-based settlement verification, and Proof of Trust attestation are all implemented through the infrastructure this extension bridges to. The extension converts the QPN's identity and trust architecture from a theoretical framework into an operationally deployed system that inherits decades of identity intelligence—and tens of billions of dollars of existing customer spend—from the vendors who have already built it.

Incremental QPN Value Add

- **Global privacy graph assembled from existing vendor investments at near-zero marginal cost** — the identity resolution that populates the graph has already been performed and paid for. The QPN adds only the cryptographic linkage layer, converting existing enterprise data management spend into a network effect.
- **Revenue-share model creating vendor adoption incentives without enterprise cost increase** — vendors earn new PNX settlement revenue from existing customer deployments; enterprises receive QPN participation and Exchange Token compensation from data they were already managing; the QPN receives a growing identity graph powered by competing vendors all contributing simultaneously.
- **Cross-domain identity linkage enabling multi-industry Exchange Networks** — healthcare identities (Datavant, HealthVerity, Synoma) linked to financial identities (LexID, Experian, TransUnion) linked to marketing identities (RampID, UID2) linked to government identities (ID.me, EUDI Wallet)—all within Privacy Domains, all privacy-preserving, all enabling settlement across domains that have never been able to share data before.
- **EasyAccess activation leveraging existing IAM deployments** — every enterprise with Okta, Entra ID, Ping, or ForgeRock can activate EasyAccess as a dual-use overlay without replacing or disrupting current identity infrastructure.
- **Real-time entity resolution eliminating identity fragmentation** — Senzing's self-correcting <200ms resolution ensures QPC identity anchors are current, linked, and disambiguated even when source data is messy or intentionally obfuscated.
- **Machine-verifiable Proof of Trust replacing manual compliance review** — attestations generated from continuous multi-vendor identity verification, entity resolution, and GRC monitoring eliminate bilateral compliance due diligence. What currently takes weeks of manual review can be generated and verified in seconds.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Trust Criteria interoperability unlocking cross-domain settlement** — semantic mappings between governance frameworks (HIPAA ↔ GDPR ↔ SOC 2 ↔ ISO 27001) enable Resources governed under one regulatory regime to satisfy Trust Block requirements defined under another.
- **Population-scale verifiable credential issuance** — EU Digital Identity Wallet (mandated for 450M+ EU citizens by 2026) and mobile driver's license infrastructure (30+ U.S. states) provide government-issued, cryptographically verifiable credentials usable as EasyAccess identity anchors without additional verification.
- **Competitive vendor dynamics driving continuous innovation** — because the QPN aggregates from competing vendors (Experian, TransUnion, and LexisNexis all resolve the same populations; Datavant and HealthVerity both tokenize healthcare data), vendors compete on resolution accuracy, coverage, and match rates to maximize their share of PNX settlement revenue. The QPN benefits from this competition without picking winners.

Target Users

Identity and access management architects, identity resolution vendors (business development and product teams), fraud prevention teams, compliance officers, KYC/AML operations, Trust Criteria authors, GRC platform administrators, EasyAccess integration engineers, decentralized identity developers, healthcare data linkage specialists, marketing data collaboration teams, entity resolution engineers, Exchange Network governance operators, and Proof of Trust attestation service providers.

Existing Installed Base

The installed base is the combined customer footprint of every vendor enumerated in this extension—and it is enormous. The three major credit bureaus (Experian, TransUnion, Equifax) collectively resolve identities for virtually every adult consumer in the United States and hundreds of millions internationally. LexisNexis LexID covers 283 million+ U.S. identities from 83 billion+ records; LexID Digital processes 35 billion+ annual transactions through the Digital Identity Network. TransUnion's OneTru platform spans 200 data sources, 16 billion monthly phone signals, and 10 billion daily digital interactions across 30+ countries. LiveRamp's AbiliTec maintains PII on 245 million U.S. individuals with 900+ global enterprise customers. UID2 is adopted across hundreds of ad tech platforms, publishers, and DSPs globally.
In healthcare, Datavant processes 60 million+ records across 80,000+ hospitals and clinics with 350+ real-world data partners and tokenization deployed in 270+ clinical trials. HealthVerity's Marketplace encompasses 150 billion+ de-identified transactions covering 330 million+ American patients from 75+ data sources. Symphony Health's IDV covers 305 million+ U.S. patients from 900,000+ data sources with 100 billion+ patient-based health transactions.
In enterprise IAM, Okta serves 18,000+ enterprise customers; Microsoft Entra ID serves 600M+ users. FIDO Alliance reports 15B+ accounts enabled for FIDO2 passkey authentication. In behavioral biometrics, BioCatch analyzes 32B+ annual sessions. The GRC market exceeds $12B annually. Identity verification is a $14.3B market in 2025 growing to $29.3B by 2030. The identity resolution software market alone exceeds $2B in 2025 growing to $5.2B+ by 2034—but this understates the true addressable base, because the QPN aggregates not just the identity resolution software spend but the resolution outputs already embedded in every enterprise's data infrastructure.

Total Addressable Value Enabled

This extension's value operates at multiple levels. First, the direct identity vendor revenue accessible through revenue-share: the combined annual revenue of the vendors enumerated in this extension exceeds $50B (credit bureaus, identity verification, entity resolution,

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

healthcare data platforms, marketing identity, GRC). The QPN's revenue share model supplements (does not replace) this spend. Second, the KYC/AML compliance cost across financial services alone exceeds $30B annually, much of it spent on redundant bilateral verification that Proof of Trust attestations can eliminate. Third, the healthcare data linkage market (where Datavant, HealthVerity, and Synoma operate) represents billions in annual spend for clinical trials, real-world evidence, and pharmaceutical commercialization that QPN-mediated settlement can monetize through Exchange Tokens.

Most consequentially, this extension enables the global privacy graph that makes multi-trillion-dollar cross-organizational data collaboration possible. Every PNX transaction requires identity resolution, trust verification, and governance attestation through the infrastructure this extension bridges to. Under the primary thesis's projections, this represents trillions in annual settlement activity flowing through the identity graph that this extension assembles from existing vendor capabilities—each settlement generating revenue share for the contributing identity vendors, creating the adoption flywheel that scales the QPN.

Development Effort Estimate

Prototype / Alpha	Controlled Beta	GA
8–12 developer-months	**14–22 developer-months**	**24–36 developer-months**

AI Development Contribution

50–65% of development is AI-assistable. IAM integration through OAuth 2.0, OIDC, and SAML is well-standardized and highly amenable to AI code generation. Senzing SDK, Datavant, HealthVerity, and LiveRamp API integrations follow documented REST patterns. Identity verification vendor APIs (LexisNexis ThreatMetrix, Jumio, Onfido) follow standard request-response patterns. GRC platform integrations (ServiceNow, OneTrust, CENTRL) are well-documented. W3C DID and Verifiable Credential handling uses established libraries. UID2 is open-source with comprehensive documentation.

The primary human effort involves: (1) Multi-vendor graph aggregation architecture—designing the privacy-preserving cross-linkage layer that connects outputs from competing vendors without any vendor seeing another's data, requiring novel cryptographic protocol design in coordination with B.13. (2) Revenue-share settlement instrumentation—engineering the attribution system that tracks which vendor's identity resolution contributed to each PNX settlement event, enabling accurate revenue-share computation across potentially dozens of contributing vendors per transaction. (3) EasyAccess dual-use overlay architecture—designing credential mapping and consent flows that transform existing enterprise logins into QPC-governed interactions without disrupting IAM operations. (4) Cross-domain Trust Criteria semantic mapping—building the governance interoperability layer across regulatory regimes. (5) Vendor business development and integration partnership—the technical work must be accompanied by commercial agreements with each vendor defining revenue-share terms, integration requirements, and data governance boundaries. The expanded GA timeline reflects the breadth of the multi-vendor ecosystem, the complexity of cross-vendor graph aggregation, the need for regulatory validation across healthcare, financial services, and marketing domains, and the commercial partnership negotiations required for each vendor tier.

B.11.15 Governance Verification & Compliance Reuse Bridge

Description

A cross-organizational compliance attestation layer that enables enterprises to prove—cryptographically and verifiably—that their existing governance infrastructure, policy enforcement systems, and compliance practices satisfy specific PNX Trust Criteria, without

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

exposing the policies themselves, the internal systems that enforce them, or the data they govern. The bridge generates machine-verifiable governance attestations by inspecting deployed access controls, classification rules, retention policies, audit configurations, encryption standards, and regulatory compliance artifacts, then producing signed evidence packages that Trust Block validators and downstream consumers can evaluate against published Trust Criteria specifications. This enables governance reuse at scale: instead of every cross-organizational collaboration requiring bilateral compliance reviews, counterparties verify governance equivalence through standardized attestations.

Capabilities

- Policy enforcement attestation — cryptographic proof that specific access control rules, classification policies, and retention schedules are actively deployed and enforced within the enterprise environment, without revealing the policies themselves.
- Regulatory compliance mapping — automated translation of enterprise compliance artifacts (SOC 2 reports, HIPAA risk assessments, GDPR DPIAs, ISO 27001 certifications) into machine-verifiable Trust Criteria satisfaction evidence.
- Continuous governance monitoring — ongoing attestation that governance conditions remain in force, with automated re-attestation on policy changes and alerting on governance state drift.
- Governance equivalence verification — enables counterparties to confirm that different enterprise governance implementations satisfy the same Trust Criteria, without requiring identical policies or identical systems.
- Audit infrastructure attestation — proof that logging, monitoring, and audit trail capabilities are operational and meet specified retention, integrity, and accessibility requirements.
- Encryption and key management attestation — verification that data-at-rest and data-in-transit encryption standards, key rotation schedules, and HSM configurations meet Trust Criteria specifications.
- Role-based access verification — proof that identity and access management systems enforce specific role hierarchies, separation-of-duty constraints, and least-privilege principles relevant to Trust Block requirements.

QPN/PNX Implementation Role

Positions existing enterprise governance infrastructure as a first-class PNX resource. Instead of treating compliance as a cost center, the bridge converts deployed governance practices into economic assets that satisfy Trust Criteria for cross-organizational settlement. This is the architectural mechanism by which the PNX inherits operational maturity from enterprises rather than requiring them to build new compliance infrastructure. Governance attestations become reusable primitives: once an enterprise proves its governance satisfies a Trust Criteria specification, that proof can be referenced by any Trust Block in any Exchange Network that requires the same standard, enabling zero-marginal-cost governance reuse across unlimited downstream settlements.

Incremental QPN Value Add

- Elimination of bilateral compliance reviews — enterprises prove governance equivalence once through standardized attestations, rather than repeating compliance due diligence for every new cross-organizational collaboration.
- Governance-as-a-Resource — enterprise compliance investment becomes a publishable, settleable PNX Resource that generates Exchange Tokens whenever downstream settlements rely on its attestations.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- Accelerated Trust Block formation — new Exchange Networks and Resource Pools form faster when participating enterprises can attest to governance readiness through machine-verifiable proofs rather than manual reviews.
- Regulatory compliance portability — enterprises operating under SOC 2, HIPAA, GDPR, ISO 27001, or sector-specific frameworks can reuse existing compliance artifacts as Trust Criteria evidence without re-certification.
- Continuous compliance assurance — ongoing monitoring and re-attestation replaces point-in-time audits, reducing governance risk for counterparties and enabling real-time Trust Block condition verification.
- Governance differentiation as competitive advantage — enterprises with stronger governance earn preferential Trust Block placement and routing priority, creating economic incentive for governance investment.

Target Users

Chief information security officers (CISOs), compliance officers, governance risk and compliance (GRC) teams, enterprise architects, audit firms (Big 4 and mid-tier), regulatory technology providers, and Trust Criteria authors.

Platforms

Integrates with GRC platforms (ServiceNow GRC, Archer, LogicGate, OneTrust, Vanta, Drata, CENTRL), identity and access management systems (Okta, Azure Entra ID, Ping Identity, SailPoint), security information and event management (Splunk, Microsoft Sentinel, CrowdStrike Falcon), cloud security posture management (Wiz, Prisma Cloud, Lacework), and regulatory compliance systems (HIPAA compliance suites, SOC 2 automation tools, GDPR management platforms).

Installed Base

The GRC market exceeds $12 billion annually and serves virtually every regulated enterprise globally. SOC 2 compliance alone covers tens of thousands of SaaS and cloud service providers. HIPAA compliance spans 60,000+ healthcare organizations in the U.S. GDPR compliance affects every enterprise serving EU data subjects. ISO 27001 certification has been issued to over 70,000 organizations worldwide. The installed base of compliance infrastructure represents one of the largest categories of enterprise software investment.

Total Addressable Value Enabled

The global cost of enterprise compliance exceeds $5 trillion annually—much of it spent on bilateral reviews, redundant audits, and manual governance verification that could be replaced by standardized, machine-verifiable attestations. Converting even 10% of this compliance overhead into reusable PNX governance attestations would represent $500 billion in direct cost savings. More significantly, the governance verification layer unlocks the multi-trillion-dollar opportunity in cross-organizational settlement that is currently blocked by compliance friction—making it the critical enabler for the full economic potential of extensions B.1 through B.13.

Development Effort & AI Leverage

Prototype	Controlled Beta	GA Release	AI-Automatable
4–6 months	**8–12 months**	**16–24 months**	**55–70%**

AI can generate substantial portions of the compliance artifact parsing, policy-to-Trust-Criteria mapping, and attestation packaging logic. GRC platform APIs are well-documented and structurally amenable to automated integration. The primary human effort involves designing

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

the governance attestation schema to be both cryptographically rigorous and interpretable by Trust Block validators, mapping heterogeneous compliance frameworks to standardized Trust Criteria specifications, and building the continuous monitoring and re-attestation pipeline. Formal verification of attestation correctness is critical and requires security engineering expertise. The timeline reflects moderate cryptographic complexity and the need for extensive validation across diverse GRC configurations.

B.11.16 AI-Powered Personalized Content & Settlement Engine

Description

An integrated AI content generation and economic settlement layer that uses agentic AI tools—Claude Code, ChatGPT Codex, GitHub Copilot, Gemini Code Assist, and equivalent systems—to automatically generate personalized web content, app experiences, communications, and multi-step workflows within Quantum Privacy Domains and Quantum Privacy Cells. The engine operates as a relying party to the EasyAccess Authorization Network and/or existing enterprise authorization systems, generating content that is privacy-preserving or fully anonymous regardless of the underlying compliance or contractual constraints. It uses crowdsourced dual-use omnichannel messaging platforms and existing engagement infrastructure to handle delivery, and tracks the utilization of every input resource—opt-ins, personal data, AI models, cloud platforms, relationships, assessments, certifications, content, and Accelerator Catalyst contributions—to support comprehensive PNX settlement and value sharing across all contributing inputs.

Capabilities

- **AI-driven personalized content generation** — agentic AI tools generate web pages, app screens, emails, messages, chatbot interactions, and multi-step workflows personalized to the recipient's context, preferences, and authorized data, all within the recipient's Quantum Privacy Domain.
- **EasyAccess relying-party integration** — the engine authenticates and authorizes through the EasyAccess Authorization Network, inheriting trust-verified consent, privacy governance, and regulatory compliance from the existing EasyAccess Consent infrastructure without requiring separate identity or authorization systems.
- **Dual-use authorization fallback** — where EasyAccess is not yet deployed, the engine integrates with existing enterprise authorization systems (OAuth 2.0, SAML, OpenID Connect) through EasyAccess's dual-use conversion capability, treating conventional identity flows as QPC-governed interactions.
- **Omnichannel delivery via dual-use infrastructure** — generated content is delivered through existing messaging platforms (email, SMS, WhatsApp, iMessage, push notifications), social channels, web properties, mobile apps, and advertising networks using their standard APIs—all operating as dual-use EasyAccess Engagement Providers at zero incremental infrastructure cost.
- **Comprehensive input resource utilization tracking** — every resource consumed in generating, personalizing, and delivering content is tracked deterministically: opt-in consents, personal data attributes, AI model invocations, cloud compute, platform infrastructure, relationship references, professional certifications, domain expertise, Accelerator Catalyst contributions, and delivery channel utilization.
- **Full-chain settlement across all inputs** — Exchange Token settlement is computed across the complete resource utilization chain, allocating proportional economic rights to every contributor: individuals whose data personalized the content, AI model providers whose models generated it, platform operators whose infrastructure delivered it,

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

professionals whose certifications validated it, and Accelerator Catalyst Contributors whose ecosystem-building work enabled it.

- **Privacy-preserving or fully anonymous interaction** — recipients interact with personalized content without revealing identity to content generators, delivery platforms, or counterparties. Personalization occurs within the recipient's QPC; the AI engine sees authorized attributes, not identity. Compliance constraints are satisfied by the governance layer, not by data exposure.
- **Crowdsourced infrastructure economics** — delivery infrastructure, AI compute, messaging platforms, and engagement surfaces are contributed by ecosystem participants operating dual-use systems. Infrastructure costs are recovered through settlement, not through centralized capital investment, enabling zero-marginal-cost scaling as the contributor network grows.

QPN/PNX Implementation Role

This extension represents the full realization of the QPN/PNX economic model at the point of interaction: AI generates personalized value, governance ensures privacy and compliance, dual-use infrastructure delivers at scale, and settlement automatically rewards every contributing resource and participant. It transforms the current model—where personalization requires data exposure, delivery requires platform lock-in, and value accrues to intermediaries—into one where personalization is privacy-preserving, delivery is crowdsourced, and value is distributed to all contributors through Exchange Token settlement. The engine is the architectural mechanism by which the QPN/PNX generates revenue at the interaction layer: every personalized content delivery event that consumes PNX Resources triggers deterministic Exchange Token issuance, creating a self-sustaining economic cycle where resource reuse generates settlement, settlement rewards contributors, and contributor rewards attract more resources.

Incremental QPN Value Add

- **Revenue generation from zero-marginal-cost reuse** — personalized content is generated by reusing and recombining existing resources (data, models, infrastructure, relationships, certifications) that have already been published to the PNX. Each interaction generates incremental settlement revenue without incremental resource acquisition cost.
- **Privacy-preserving personalization at scale** — AI generates highly personalized content using authorized attributes within Quantum Privacy Domains, delivering precision personalization without the privacy violations, regulatory risk, and consumer backlash associated with current surveillance-based personalization.
- **Fully anonymous interaction capability** — individuals can receive and act on personalized content without revealing identity to any external party, enabling engagement in sensitive domains (healthcare, financial counseling, crisis support, whistleblowing, political participation) where anonymity is essential.
- **Universal value sharing across all inputs** — every participant in the content generation and delivery chain—from the individual whose opt-in enabled the interaction, to the AI model that generated the content, to the Accelerator Catalyst contributor whose ecosystem work made the Exchange Network possible—receives proportional Exchange Token settlement.
- **Crowdsourced infrastructure eliminating capital requirements** — delivery uses existing dual-use messaging, web, and app infrastructure contributed by ecosystem participants. No centralized build-out is required. Infrastructure costs are recovered through settlement at the margin, not through upfront capital investment.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Accelerator Catalyst contribution monetization** — ecosystem-building work captured through the Accelerator Catalyst (introductions, advocacy, technical validation, governance frameworks, infrastructure contributions) earns settlement revenue whenever the Exchange Networks those contributions helped create generate personalized content deliveries.
- **Competitive displacement of surveillance-based advertising** — privacy-preserving personalization that is more effective (because it uses authorized, accurate data rather than inferred profiles), more compliant (because governance is embedded in the architecture), and more economically efficient (because zero-marginal-cost reuse eliminates the per-interaction data acquisition cost that dominates advertising economics).

Target Users

AI application developers, digital marketing technologists, enterprise communication architects, healthcare engagement platforms, financial services advisors, government citizen services teams, e-commerce personalization engineers, creator economy platforms, Accelerator Catalyst Contributors, Solution Providers, and Exchange Network operators.

Platforms

AI generation: Claude Code, ChatGPT/Codex, GitHub Copilot, Gemini Code Assist, open-source LLMs deployed within Privacy Domains. **Delivery**: existing omnichannel infrastructure including email (SendGrid, Mailgun, Amazon SES), **SMS/messaging** (Twilio, Vonage, MessageBird), **push notifications** (Firebase, OneSignal), **social platforms** (Meta, X/Twitter, LinkedIn APIs), **web content delivery** (Cloudflare, Akamai, Vercel), **advertising networks** (Google Ads, The Trade Desk, Meta Ads), and **enterprise platforms** (Salesforce Marketing Cloud, HubSpot, Braze). **Authorization**: EasyAccess Authorization Network, plus dual-use integration with existing OAuth 2.0/OIDC/SAML providers.

Installed Base

The combined installed base encompasses virtually the entire digital interaction surface. AI coding and content generation tools are used by tens of millions of developers and content creators. Omnichannel messaging platforms deliver hundreds of billions of messages monthly. Advertising networks reach over 4 billion internet users. E-commerce platforms process trillions in annual transactions. Healthcare, financial, and government engagement platforms serve billions of individuals globally. Every organization that operates a website, mobile app, or messaging channel is a potential dual-use infrastructure contributor.

Total Addressable Value Enabled

This extension addresses the broadest economic surface of any in the appendix because it operates at the point where resources are consumed and value is created: the personalized interaction. Global digital advertising exceeds $1 trillion annually, but is limited to attention monetization. Global e-commerce exceeds $6 trillion. Healthcare, financial, and government service delivery collectively exceed $20 trillion. Personalized AI-mediated interaction within these domains—with full privacy preservation and universal value sharing—represents an addressable value layer of $10–50 trillion annually as AI-driven personalization replaces static content delivery across every sector. The zero-marginal-cost reuse economics mean that revenue scales with interaction volume, not with infrastructure investment, creating the potential for the highest-margin, highest-scale settlement flows in the PNX ecosystem.

Development Effort & AI Leverage

Prototype	Controlled Beta	GA Release	AI-Automatable

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

6–9 months	**12–18 months**	**20–30 months**	**70–85%**

This extension has the highest AI development leverage in the appendix because the core capability—generating personalized content—is exactly what agentic AI tools are designed to do. AI can generate the content generation pipelines, the personalization logic, the delivery orchestration, and much of the settlement computation. The primary human effort involves EasyAccess Authorization integration architecture, privacy-preserving personalization within Quantum Privacy Domains (ensuring AI models operate on authorized attributes without identity exposure), settlement accounting across complex multi-input resource chains, and compliance validation across heterogeneous regulatory regimes. The delivery layer is largely solved: omnichannel messaging and content delivery infrastructure is mature, well-documented, and highly amenable to AI-assisted integration. The novel engineering challenge is the settlement layer—tracking every input resource utilization and computing proportional Exchange Token allocation across potentially hundreds of contributing resources per interaction.

B.11.17 Quantum Rating System Infrastructure

Description

A domain-neutral rating infrastructure that enables the creation, management, auditing, and evolution of trustworthy Quantum Rating Schemes within the QPN/PNX. The system does not prescribe specific rating criteria—which vary by domain, jurisdiction, use case, and community—but provides the foundational mechanisms for defining, computing, verifying, and enforcing multi-dimensional ratings across participants, resources, transactions, and trust relationships while preserving privacy and preventing gaming, manipulation, or coercion. The infrastructure operates within Quantum Privacy Domains and under Trust Block governance, ensuring that ratings are computed on authorized attributes without exposing the underlying data to rated parties, rating consumers, or rating system operators themselves. Rating computations produce verifiable, lineage-linked attestations that can be audited for fairness, accuracy, and methodology compliance—without revealing the inputs.
This extension connects to Patent Group 5 (Quantum Rating System, Claims 131–165), which claims the Core Quantum Rating Engine, Lineage-Aware Multi-Dimensional Rating Models, and Cross-Domain Rating Normalization, Routing & Policy Alignment.

Capabilities

- **Rating Scheme Definition Framework** — a structured, machine-interpretable specification language for defining Quantum Rating Schemes. Each scheme specifies rated entity types, input attributes (with privacy classifications), computational methodology, output dimensions, update frequency, governance rules, dispute resolution procedures, and Trust Criteria requirements. Schemes are versioned, published to the Unified Trust Model, and subject to Proof of Trust accreditation before activation.
- **Privacy-preserving rating computation** — computes ratings within Quantum Privacy Domains using authorized attributes from rated entities' QPCs. Zero-knowledge proof circuits enable rating consumers to verify that a rating was computed correctly according to the published scheme methodology without seeing the inputs. Homomorphic computation enables aggregate ratings across populations without decrypting individual records.
- **Lineage-aware multi-dimensional rating models** — ratings are not scalar scores but multi-dimensional trust profiles linked to the lineage of every input that contributed to the computation. When a rating changes, the lineage identifies which input changes drove the

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

update. When a rating is disputed, the lineage supports auditable reconstruction without exposing privacy-protected data.

- **Cross-domain rating normalization and interoperability** — enables ratings computed under different schemes, in different domains, and by different operators to be compared, aggregated, and routed through Exchange Networks. A healthcare quality rating and a financial creditworthiness rating cannot be directly compared, but the normalization infrastructure expresses both in terms of their respective Trust Criteria compliance and methodological rigor, enabling composite trust assessments across domains.
- **Anti-gaming and manipulation resistance** — structural protections against rating manipulation including Sybil resistance (preventing fake entity creation to inflate ratings), collusion detection (identifying coordinated rating behavior), temporal smoothing (preventing rapid rating oscillation through short-term behavior changes), and cryptographic commitment schemes that prevent rated entities from selectively revealing favorable inputs.
- **Rating governance and accountability** — every rating scheme operates under published governance rules specifying who can create, modify, or retire the scheme; how disputes are adjudicated; what appeals processes exist; and how methodological changes are versioned and communicated. Rating scheme governance is itself subject to AGPW-weighted policy constraints, preventing any single authority from imposing rating criteria that violate participants' rights.

QPN/PNX Implementation Role

The Quantum Rating System is the trust signaling infrastructure that enables efficient routing, matching, and pricing across the PNX. Without trustworthy ratings, Exchange Networks cannot efficiently allocate resources, participants cannot assess counterparty reliability, and the PPOS matching engine cannot optimize multi-criteria selections. Every Extension Bridge that publishes resources to the PNX (B.1–B.10) produces rated resources; every identity resolution adapter (B.14) produces rated identity matches; every governance verification (B.15) produces rated compliance attestations. The QRS infrastructure provides a common framework for creating, managing, and consuming all these domain-specific ratings.

Incremental QPN Value Add

- **Trustworthy, privacy-preserving rating infrastructure** — structurally superior to existing rating systems because it operates on verified, lineage-linked data within Quantum Privacy Domains rather than on self-reported or surveilled data.
- **Cross-domain rating normalization** — enables composite trust assessments spanning multiple domains that no single-domain rating system can produce.
- **Anti-gaming protections** — address the fundamental vulnerabilities of existing reputation systems through cryptographic commitment, Sybil resistance, and collusion detection.
- **Decentralized rating governance** — prevents rating monopolies and conflicts of interest that undermine trust in conventional rating agencies.
- **Rating-as-a-Resource economics** — rating scheme creation and operation generates Exchange Token settlement, converting trust assessment from a cost center into an economically productive PNX activity.

Target Users

Exchange Network operators, Trust Criteria architects, compliance engineers, risk management professionals, marketplace designers, identity verification specialists, healthcare quality measurement organizations, financial rating analysts, ESG rating providers, and any domain expert designing trust assessment frameworks for their sector.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Platforms

Credit rating and scoring infrastructure: FICO, VantageScore, Dun & Bradstreet, Moody's Analytics, S&P Global Ratings data feeds. Reputation and trust systems: platform reputation engines (eBay, Amazon, Airbnb seller ratings), professional credentialing systems, peer review systems. Identity and risk scoring: LexisNexis Risk Solutions, Experian, TransUnion, Socure, Prove. ESG and sustainability rating providers: MSCI ESG, Sustainalytics, CDP, ISS ESG. Healthcare quality: CMS Star Ratings, HEDIS, Leapfrog, Press Ganey. Compliance rating: SOC 2, ISO 27001, FedRAMP, HITRUST certifications.

Installed Base

The global credit rating industry manages ratings for over $130 trillion in rated debt. Consumer credit scoring covers 200M+ scored individuals in the U.S. alone. Platform reputation systems operate at billions-of-ratings scale. Healthcare quality measurement systems rate 6,000+ hospitals and hundreds of thousands of providers. ESG rating systems assess 10,000+ companies globally. Each operates within its domain silo with incompatible methodologies, opaque inputs, and no cross-domain interoperability—the exact limitations the QRS infrastructure addresses.

Total Addressable Value Enabled

Rating infrastructure is a prerequisite for efficient exchange rather than a direct revenue generator. Its value is measured by the settlement efficiency it enables across the PNX. Trustworthy ratings reduce friction in every transaction by enabling faster counterparty assessment, more accurate pricing, and more efficient resource matching. The differential value between a PNX with trustworthy cross-domain ratings and a PNX without them is conservatively estimated at 10–30% of total settlement volume—representing hundreds of billions to trillions in enabled value annually at scale.

Development Effort & AI Leverage

Prototype	Controlled Beta	GA Release	AI-Automatable
6–10 dev-months	**10–16 dev-months**	**18–26 dev-months**	**55–70%**

AI can generate the bulk of the rating scheme definition language parsing, zero-knowledge proof circuit scaffolding, normalization algorithms, and API integrations with existing rating platforms. The primary human effort involves cryptographic protocol design for privacy-preserving rating computation, anti-gaming mechanism design requiring game theory expertise, governance framework specification, and cross-domain normalization methodology—areas requiring specialized expertise in mechanism design, applied cryptography, and formal trust modeling.

B.11.18 QPC Lifecycle Automation & Propagation

Description

The automated lifecycle management system for Quantum Privacy Cells (QPCs) at population scale—encompassing creation, activation, suspension, retirement, interdependency management, entanglement propagation, and dynamic reallocation. This extension provides the core runtime that transforms QPCs from static governance containers into dynamic, self-managing entities that respond to changing conditions, propagate rights and obligations through dependency chains, and maintain compliance across their full lifecycle without manual intervention.

The system manages QPCs for individuals, enterprises, AI agents, devices, and institutional entities—potentially billions of concurrent QPCs with complex interdependency graphs

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

spanning multiple jurisdictions, governance domains, and trust frameworks. It operates within the privacy-preserving architecture of the QPN, ensuring that lifecycle operations on one QPC do not reveal information about other QPCs or the dependency relationships between them. This extension connects to Patent Group 4 (QPC Lifecycle Automation & Propagation Mechanisms, Claims 86–130), which claims Automated QPC Creation, Activation, Suspension & Retirement; QPC Interdependency, Entanglement & Propagation; and Population-Scale QPC Governance, Monitoring & Dynamic Reallocation.

Capabilities

- **Automated QPC creation** — instantiates QPCs for individuals, enterprises, AI agents, and devices through the EasyAccess consent process. QPC creation includes legal entity formation (Series LLC compartment or equivalent), cryptographic key generation and escrow, Privacy Domain initialization, Trust Criteria binding, and initial trust credential provisioning. Supports both interactive creation (user-initiated) and batch creation (population-scale enrollment through platform integration).
- **State machine lifecycle management** — manages QPCs through defined lifecycle states: DORMANT (created but not activated), ACTIVE (fully operational), SUSPENDED (temporarily restricted due to compliance review, dispute, or participant request), RESTRICTED (operational with reduced capabilities pending resolution), and RETIRED (permanently deactivated with lineage preservation). State transitions are governed by Trust Criteria, triggered by events, and recorded as immutable Trust Blocks.
- **QPC interdependency and entanglement propagation** — manages the dependency graph between QPCs. When a parent QPC's state changes (e.g., an enterprise QPC is suspended), the system automatically propagates appropriate state changes to dependent QPCs (employee QPCs, delegated authority QPCs, AI agent QPCs) according to dependency rules defined in Trust Criteria. Entanglement rules specify how rights, obligations, and constraints flow through dependency chains—enabling complex organizational governance without manual coordination.
- **Population-scale monitoring and dynamic reallocation** — continuously monitors QPC compliance across the entire population using Trust Criteria evaluation. Detects and responds to compliance events (jurisdiction changes, regulatory updates, consent revocations, trust credential expirations) automatically. Dynamically reallocates resources, rights, and obligations across QPC populations in response to changing conditions.
- **Cryptographic key lifecycle** — manages the full lifecycle of cryptographic keys associated with QPCs: generation, rotation, escrow, recovery, and revocation. Integrates with hardware security modules (HSMs), key management services (AWS KMS, Azure Key Vault, Google Cloud KMS), and post-quantum key exchange protocols (B.13). Supports key recovery through multi-party computation and social recovery mechanisms without exposing keys to any single party.
- **Cross-jurisdiction lifecycle coordination** — manages QPCs that operate across multiple jurisdictions with potentially conflicting regulatory requirements. Automatically applies the most restrictive applicable requirements, manages jurisdiction-specific consent flows, and ensures that lifecycle operations respect the data sovereignty constraints of all relevant jurisdictions.

QPN/PNX Implementation Role

QPC Lifecycle Automation is the operational backbone of the entire QPN. Every participant in the network—individual, enterprise, AI agent, device—is represented by a QPC. Without automated lifecycle management, the network cannot enroll participants at scale, cannot

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

maintain compliance as conditions change, cannot propagate governance decisions through organizational hierarchies, and cannot retire or suspend QPCs when required by law or policy. This extension is not an optimization; it is a prerequisite for the QPN to function as a production system beyond manually managed pilot deployments.

Incremental QPN Value Add

- **Population-scale participant management** — enables the QPN to operate with billions of concurrent QPCs without manual lifecycle intervention.
- **Compliance automation** — ensures that every QPC in the network maintains continuous compliance with all applicable Trust Criteria—a capability no existing identity or governance system provides at this scale.
- **Dependency propagation** — enables complex organizational governance (enterprise hierarchies, supply chains, contractual relationships) to be enforced automatically through QPC entanglement rather than manual policy administration.
- **Cryptographic key resilience** — ensures participant access and sovereignty survive device loss, key compromise, and infrastructure migration through multi-party recovery mechanisms.

Target Users

Core QPN runtime engineers, Privacy Domain operators, EasyAccess infrastructure architects, enterprise identity management teams, compliance automation engineers, legal entity management specialists, and cryptographic key management architects.

Platforms

Identity and access management: Okta, Microsoft Entra ID, Ping Identity, ForgeRock, Auth0. Legal entity management: CT Corporation, CSC Global, Cogency Global for Series LLC lifecycle automation. Smart contract platforms: Hedera Smart Contract Service, Ethereum/Solidity, Hyperledger Fabric. Cloud orchestration: Kubernetes, Terraform, Pulumi. Workflow engines: Temporal, Apache Airflow, AWS Step Functions. Key management: AWS KMS, Azure Key Vault, Google Cloud KMS, Thales HSMs.

Installed Base

Enterprise identity lifecycle management (Okta, Entra ID, Ping) manages hundreds of millions of identity records with automated provisioning and deprovisioning. Cloud orchestration platforms (Kubernetes, Terraform) manage billions of infrastructure lifecycle events daily. Smart contract platforms (Hedera, Ethereum) manage millions of on-chain entity states. The QPC Lifecycle system extends these proven patterns to the governance-container lifecycle that the QPN uniquely requires.

Total Addressable Value Enabled

As foundational runtime infrastructure, this extension enables the entire PNX settlement volume. Without it, QPC creation and management must be manual, limiting the network to thousands of participants rather than billions. The delta between manual and automated QPC lifecycle management represents the difference between a pilot system and a global production network—the full projected PNX settlement volume is gated on this capability.

Development Effort & AI Leverage

Prototype	Controlled Beta	GA Release	AI-Automatable
8–12 months	**14–22 months**	**24–36 months**	**50–65%**

AI can generate state machine implementation, API integrations with identity platforms, cloud orchestration patterns, and monitoring infrastructure. The primary human effort involves

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

cryptographic key lifecycle design, entanglement propagation rule specification, cross-jurisdiction compliance logic, and formal verification of lifecycle state machine correctness—areas requiring deep expertise in distributed systems, applied cryptography, and regulatory compliance engineering.

B.11.19 EasyAccess Deployment Infrastructure

Description

The deployable production system implementing EasyAccess Authorization, EasyAccess Links, EasyAccess Messaging, and EasyAccess Rewards as operational services that enable population-scale consent, enrollment, engagement, and privacy-preserving interaction between participants and the QPN/PNX. EasyAccess is the adoption layer of the Quantum Privacy Network—the mechanism through which people, organizations, and systems connect to and participate in the Privacy Network Exchange at near-zero marginal cost without requiring app downloads, account creation, system integration, or IT involvement.

A demonstrable prototype of this system already exists, validating the core architectural patterns. This extension brings that prototype to production-grade deployment at population scale.

This extension connects to Patent Group 3 (EasyAccess Infrastructure, Claims 64–85), which claims EasyAccess Links & Zero-Integration Activation, Dual-Use Conversion of Apps/APIs/Platforms, and EA Messaging, Social Propagation & Viral Routing.

Capabilities

- **EasyAccess Consent API** — a lightweight REST/GraphQL API implementing the consent, delegation, policy enforcement, and rights assertion flows described in Appendix A.1. Enables any application or platform to become an EasyAccess Engagement Network by adding a single API integration. The API handles PPN creation or connection, QPC consent recording, Trust Criteria binding, and session token issuance—reducing integration effort to hours of development time and a minimal Privacy Statement update.
- **EasyAccess Link generation and routing engine** — generates privacy-preserving, context-aware links embeddable in any digital medium: web pages, emails, SMS, QR codes, NFC tags, advertising creatives, social media posts, documents, and physical media. Each link encodes the minimum necessary context (target Resource, consent scope, routing hints) while revealing nothing about the participant, the Resource, or the PNX infrastructure to intermediaries. Links are self-contained: clicking on any device, in any browser, without pre-installed software initiates the consent flow and connects the participant to the PNX.
- **EasyAccess Messaging infrastructure** — persistent, privacy-preserving, omni-channel messaging enabling participants to communicate through their QPCs. Messages are routed through the sender's PPN, encrypted end-to-end, and delivered through the recipient's preferred channel (email, SMS, in-app notification, messaging platform) without either party needing to know the other's contact information. Supports both human-to-human and agent-to-human communication.
- **EasyAccess Rewards engine** — converts engagement events (link clicks, consent grants, resource access, referrals, content sharing) into verifiable contribution records that accrue Quantum Privacy Rewards. Every EasyAccess interaction generates measurable economic value recorded as encrypted Trust Blocks, turning participation itself into a compensated activity. Integrates with the Accelerator Catalyst attribution system (Capture Tools).
- **Viral propagation mechanics** — structural features that make EasyAccess Links inherently viral: link recipients can reshare to their own networks, each reshare is attribution-tracked (the resharer earns Quantum Privacy Rewards for downstream engagement they enable), and network effects compound as each new participant's connections become reachable through the PNX.
- **Platform dual-use conversion** — enables existing platforms and applications to become EasyAccess Engagement Networks through minimal integration. A platform operator adds the EasyAccess Consent API, updates its Privacy Statement per the redlines in Appendix A.2, and its

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

entire user base becomes enrollable in Personal Privacy Networks. The platform continues operating exactly as before—the QPN layers privacy-preserving exchange capability on top. This is the mechanism by which a single major platform integration (Meta, Google, Microsoft, Amazon) can batch-enroll hundreds of millions to billions of users.

QPN/PNX Implementation Role

EasyAccess is the single most important adoption mechanism in the QPN architecture. Without it, participant enrollment requires bespoke integration, manual onboarding, and platform-specific development for every touchpoint. With it, enrollment is as simple as clicking a link, scanning a QR code, or responding to a message. EasyAccess transforms the QPN from a system that organizations must deliberately adopt into a system that propagates through existing communication and engagement patterns. The difference between the QPN with and without production EasyAccess infrastructure is the difference between a specialized enterprise platform and a universal participation layer.

Incremental QPN Value Add

- **Near-zero-friction enrollment** — enables population-scale participation without app downloads, account creation, or IT involvement.
- **Universal channel coverage** — reaches participants through whatever digital medium they already use—email, SMS, web, QR codes, messaging apps, social media, advertising.
- **Viral propagation** — converts every enrolled participant into a potential enrollment vector for their network, with attribution-tracked incentives for resharing.
- **Platform dual-use conversion** — enables billion-user platforms to become QPN enrollment channels through hours of integration effort.
- **Attribution-tracked engagement** — converts participation itself into an economically compensated activity through Quantum Privacy Rewards.
- **Existing prototype validation** — core architectural patterns are already demonstrated, reducing development risk and accelerating time to production deployment.

Target Users

Platform integration engineers, consumer product architects, marketing technology specialists, mobile developers, enterprise application developers, messaging infrastructure engineers, and any technology team seeking to connect their platform or user base to the QPN/PNX.

Platforms

Authentication and authorization: OpenID Connect/OAuth 2.0 providers (Google, Microsoft, Apple, Facebook login), FIDO2/WebAuthn biometric authentication, passkeys. Messaging: email (SMTP/IMAP), SMS/MMS, WhatsApp Business API, Slack, Microsoft Teams, RCS. Web and mobile: standard browsers (via EasyAccess Links), mobile deep linking (iOS Universal Links, Android App Links), progressive web apps. Advertising and content distribution: Google Ads, Meta Ads, The Trade Desk, CMS platforms (WordPress, Drupal, Shopify), email marketing (Mailchimp, Salesforce Marketing Cloud). Enterprise: CRM systems (Salesforce, HubSpot, Dynamics), HR platforms (Workday, ADP), customer support (Zendesk, ServiceNow).

Installed Base

OAuth 2.0/OpenID Connect identity infrastructure serves billions of authentication events daily across virtually every web and mobile application. Email reaches 4+ billion accounts globally. SMS/MMS reaches 5+ billion mobile subscribers. Social media platforms collectively serve 5+ billion monthly active users. QR code scanning is native to every modern smartphone camera. EasyAccess leverages all of this existing infrastructure rather than competing with it.

Total Addressable Value Enabled

EasyAccess's addressable value equals the total PNX settlement potential, because EasyAccess is the mechanism by which participants connect to the PNX. Under the primary thesis projections, this represents trillions in annual settlement. More precisely, EasyAccess is the rate-limiting factor for

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

enrollment velocity—every month of faster enrollment translates to earlier settlement revenue, earlier Quantum Privacy Rewards distribution, and earlier cascading adoption. This makes EasyAccess development the highest-ROI investment in the entire Extension Bridge portfolio.

Development Effort & AI Leverage

Prototype	Controlled Beta	GA Release	AI-Automatable
5–8 months	**10–16 months**	**18–26 months**	**65–80%**

This extension benefits from an existing demonstrable prototype that validates core architectural patterns, significantly reducing development risk. AI can generate REST/GraphQL API implementations, OAuth/OIDC integrations, link generation, messaging routing, and channel-specific delivery adapters—all well-structured engineering tasks. The primary human effort involves cryptographic protocol design for privacy-preserving link routing, abuse prevention and anti-spam mechanisms, cross-channel delivery reliability engineering, and the security review required for a system that handles population-scale consent and identity flows.

B.11.20 Exchange Network & Resource Pool Runtime

Description

The core operational runtime of the Privacy Network Exchange (PNX)—the system that creates, manages, and operates Exchange Networks and Resource Pools, performs trust-verified clearing and settlement, routes resources between pools, and enforces the governance constraints that make privacy-preserving cross-organizational exchange possible. This is the PNX's execution engine: the system that converts published resources (from B.1–B.10), enrolled participants (via B.18 and B.19), and trust assessments (from B.15 and B.17) into actual economic settlement events that generate Exchange Token value.

The runtime manages the full lifecycle of Exchange Networks (creation, configuration, resource admission, participant enrollment, settlement execution, governance enforcement, retirement) and Resource Pools (pool formation, resource contribution, virtual pooling, regeneration, cloning, hybridization, and value distribution). It operates within the privacy-preserving architecture of the QPN, ensuring that settlement occurs without revealing participant identities, resource contents, or transaction terms to any party not authorized by the governing Trust Criteria.

This extension connects to Patent Group 8 (Exchange Networks, Resource Pools & Trust-Verified Tokenization, Claims 256–305), which claims Resource Tokens & Provenance-Governed Allocation, Exchange Networks & Trust-Verified Clearing, and Multi-Pool Coordination & Liquidity Routing.

Capabilities

- **Exchange Network lifecycle management** — creates, configures, and operates Exchange Networks as governed marketplaces within the PNX. Each Exchange Network defines its resource types, participant eligibility, Trust Criteria requirements, settlement mechanics, and governance rules. Networks can be domain-specific (healthcare data exchange, financial instrument clearing), cross-domain (linking healthcare and financial data through identity resolution), or universal (open to any resource type meeting minimum trust requirements).
- **Resource Pool formation and virtual pooling** — enables resources from multiple contributors to be virtually combined into pools without physical data movement or duplication. A healthcare Resource Pool might virtually combine clinical data from 50 hospital systems, each retaining custody and governance control, while making the aggregate analytically available as a single governed resource. Pool formation respects all contributing resources' Trust Criteria, and settlement flows automatically to all contributors proportional to their resource's role in value generation.
- **Resource Pool regeneration, cloning, and hybridization** — enables pools to generate derivative resources (analytics, models, insights, processed datasets) that themselves become poolable resources. A clinical data pool generates a trained AI model; that model is contributed to a model

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

pool; the model pool generates inference services; those services settle independently—with value flowing back through the full lineage chain to every original data contributor.

- **Trust-verified clearing and settlement** — executes settlement events by verifying that all Trust Criteria governing all resources, participants, and governance domains involved in the transaction are satisfied; computing Exchange Token distribution across all contributing parties; recording settlement as immutable Trust Blocks; and issuing or transferring Exchange Tokens through the B.12 Token Platform Bridge. Settlement is atomic: either all Trust Criteria are satisfied and all parties are settled, or the transaction does not execute.
- **Multi-pool coordination and liquidity routing** — routes settlement across multiple Resource Pools and Exchange Networks to satisfy complex transactions that span domains. A pharmaceutical company's real-world evidence query might draw from a clinical data pool, a claims data pool, a pharmacy dispensing pool, and a patient-reported outcomes pool—each governed by different Trust Criteria, operated by different organizations, and subject to different regulatory requirements. The runtime coordinates settlement across all pools as a single logical transaction.
- **Governance constraint enforcement** — enforces all Trust Criteria, access policies, usage restrictions, revenue-sharing rules, and compliance requirements at the settlement layer. No resource can be accessed, no data can be linked, no model can be trained, and no settlement can occur unless the runtime verifies that every applicable governance constraint is satisfied. Compliance is structural rather than procedural—violations are architecturally impossible, not merely policy-prohibited.

QPN/PNX Implementation Role

This extension IS the PNX. All other extensions publish resources to it (B.1–B.10), manage participants within it (B.18, B.19), assess trust for it (B.15, B.17), provide cryptographic infrastructure beneath it (B.13), resolve identities across it (B.14), provide liquidity for its tokens (B.12), and compute pricing within it (B.11). The Exchange Network & Resource Pool Runtime is the system that takes all of these components and produces actual economic settlement. Without it, the QPN has infrastructure but no exchange.

Incremental QPN Value Add

- **Zero-marginal-cost resource reuse across organizational boundaries** — the fundamental economic innovation of the PNX. Virtual pooling without data movement eliminates infrastructure cost. Automated multi-party settlement eliminates transaction cost. Trust-verified clearing eliminates compliance cost.
- **Lineage-preserving value distribution** — every settlement event automatically distributes Exchange Tokens to all upstream contributors through the full Resource lineage chain, ensuring that original data providers, model trainers, infrastructure contributors, and governance attestors are compensated regardless of how many intermediate pools and derivatives their resources pass through.
- **Atomic, trust-verified settlement** — eliminates settlement risk and governance ambiguity by making compliance verification and economic settlement a single atomic operation. No counterparty trust required—the runtime enforces governance mathematically.
- **Cross-domain exchange** enables economic settlement between domains that have never been able to transact directly due to incompatible governance, different regulatory regimes, or an absence of trust infrastructure.

Target Users

Core PNX runtime engineers, Exchange Network operators, Resource Pool architects, settlement infrastructure engineers, smart contract developers, distributed systems architects, and enterprise integration teams connecting organizational resources to the PNX.

Platforms

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Distributed ledger and consensus: Hedera Consensus Service and Token Service, Ethereum/L2s for cross-chain interoperability. Data exchange: Databricks DeltaShares, Snowflake Data Sharing, AWS Data Exchange, Google Analytics Hub. Compute orchestration: Kubernetes, Apache Spark, Ray. Event streaming: Apache Kafka, AWS Kinesis, Google Pub/Sub, Azure Event Hubs. Smart contracts: Hedera Smart Contract Service, Solidity/EVM.

Installed Base

Financial exchange and clearing infrastructure (DTCC, CLS, Euroclear) processes trillions daily with proven settlement mechanics. Data exchange platforms (Databricks DeltaShares, Snowflake Sharing) handle cross-organizational data access at enterprise scale. Event streaming platforms (Kafka, Kinesis) process billions of events daily. DeFi protocols (Uniswap, Aave, Compound) demonstrate automated, trustless settlement at global scale. The PNX runtime synthesizes patterns from all of these into a unified, privacy-preserving, trust-verified exchange engine.

Total Addressable Value Enabled

The Exchange Network & Resource Pool Runtime enables the full PNX settlement volume. Under the primary thesis projections, this represents trillions in annual settlement growing to tens of trillions at scale. The runtime is the direct revenue-generating component of the QPN—every Exchange Token issued, every settlement event recorded, every value distribution computed flows through this system.

Development Effort & AI Leverage

Prototype	Controlled Beta	GA Release	AI-Automatable
10–14 months	**16–24 months**	**28–40 months**	**45–60%**

AI can generate API integrations with data exchange and ledger platforms, event processing pipelines, smart contract implementation, and settlement computation logic. The primary human effort involves distributed consensus and atomicity guarantees for cross-pool settlement, cryptographic protocol design for privacy-preserving clearing, formal verification of settlement correctness and governance enforcement, and the system reliability engineering required for financial-grade infrastructure—areas requiring deep expertise in distributed systems, applied cryptography, and financial systems engineering.

B.11.21 Unified Trust Model Runtime & Trust Taxonomy Management

Description

The operational runtime implementing the Unified Trust Model (UTM) as a production system—managing Trust Criteria ontologies, Trust Credential lifecycle, Trust Enforcement logic, Ownership Rights mappings, and Resource Trust taxonomies as live, queryable, evolvable infrastructure. The UTM Runtime is the system that transforms legal, regulatory, fiduciary, contractual, and ethical obligations into machine-interpretable, machine-enforceable policy logic that every other QPN component relies upon for governance decisions.

The runtime manages five core ontologies: the Trust Criteria Ontology (defining what must be satisfied), the Trust Credential Ontology (defining how satisfaction is attested), the Trust Enforcement Ontology (defining how constraints are applied), the Ownership Rights Ontology (defining who holds what rights), and the Resource Trust Ontology (defining what resources can be used under what conditions). These ontologies are not static taxonomies—they evolve continuously as regulations change, jurisdictions update requirements, and communities develop domain-specific trust frameworks.

This extension connects to the Unified Trust Model, Proof of Trust, and Adaptive Accreditation specifications described in Quantum Privacy Network-Universal Exchange, Ownership & AI, Sections 2.6–2.10 and to the trust infrastructure claims across all three provisional patents.

Capabilities

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Trust Criteria compilation** — transforms human-readable legal, regulatory, and contractual requirements into machine-interpretable Trust Criteria evaluable programmatically at every governance decision point. A HIPAA requirement becomes a computable predicate; a GDPR consent requirement becomes a verifiable constraint; a contractual data-use limitation becomes an enforceable access policy. The compiler supports natural language input (with AI-assisted parsing), structured input (from regulatory databases), and formal input (from policy specification languages).
- **Trust Taxonomy management** — maintains the five UTM ontologies as living, versioned, collaboratively governed knowledge structures. Proposed changes are submitted, reviewed against consistency constraints, impact-assessed for downstream effects, and either adopted (with version increment) or rejected. Taxonomy changes automatically propagate to all dependent Trust Criteria, Trust Credentials, and enforcement logic—ensuring consistency as the regulatory and contractual landscape evolves.
- **Cross-domain trust mapping** — enables trust assessment across domains that use different Trust Criteria, different credential formats, and different enforcement mechanisms. A healthcare compliance attestation and a financial services audit report cannot be directly compared, but the UTM Runtime expresses both in terms of common ontological primitives (what was assessed, by whom, using what methodology, against what standard) enabling cross-domain trust inference without requiring a single universal standard.
- **Proof of Trust accreditation engine** — evaluates entities (organizations, platforms, services, individuals) against specified Trust Criteria and issues Trust Credentials attesting to the evaluation result. Supports self-assessment, peer assessment, expert assessment, automated assessment (through integration with compliance monitoring platforms), and continuous assessment (ongoing monitoring rather than point-in-time audits). Accreditation results are recorded as Trust Blocks with full lineage.
- **Adaptive trust evolution** — monitors the regulatory, legal, and contractual landscape for changes that affect active Trust Criteria. When a regulation changes, the runtime identifies all affected Trust Criteria, Trust Credentials, and participants, then initiates re-evaluation workflows, notifies affected participants, and enforces updated requirements—ensuring the QPN adapts to regulatory change in near-real-time rather than through periodic manual compliance reviews.
- **Trust Criteria API** — exposes UTM functionality as queryable services for all other QPN components. The Exchange Network Runtime (B.20) queries Trust Criteria to verify settlement eligibility. The QPC Lifecycle system (B.18) queries Trust Criteria to determine lifecycle state transitions. The Quantum Rating System (B.17) queries Trust Criteria for rating scheme compliance requirements. EasyAccess (B.19) queries Trust Criteria to determine consent scope. Every governance decision in the QPN ultimately resolves to a Trust Criteria query processed by this runtime.

QPN/PNX Implementation Role

The UTM Runtime is the governance substrate upon which the entire QPN operates. It is to the QPN what the legal system is to a national economy—the framework within which all transactions, all relationships, and all enforcement actions are evaluated and authorized. Without it, every governance decision requires manual evaluation by a human expert, limiting the QPN to manually governed pilot deployments. With it, governance is automated, consistent, auditable, and scalable to billions of concurrent QPCs operating across every jurisdiction and domain.

Incremental QPN Value Add

- **Machine-interpretable compliance** — converts legal and regulatory requirements from documents humans read into constraints software enforces—the fundamental capability that makes automated, compliant exchange possible.
- **Cross-domain trust mapping** — enables exchange between domains that have never been able to share data due to incompatible compliance frameworks.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Adaptive trust evolution** — ensures the QPN automatically adjusts to regulatory changes rather than requiring manual compliance updates.
- **Proof of Trust automation** — reduces accreditation from months-long manual audit processes to continuous, evidence-based assessment.
- **Governance-as-infrastructure economics** — Trust Criteria authorship, Trust Credential issuance, and compliance assessment generate Exchange Token settlement, converting governance from cost center to economically productive PNX activity.

Target Users

Trust Criteria architects, compliance engineers, regulatory affairs specialists, legal technology professionals, policy engine developers, ontology engineers, Proof of Trust assessors, and any domain expert translating sector-specific governance requirements into machine-interpretable Trust Criteria.

Platforms

Ontology and knowledge management: OWL/RDF frameworks, Apache Jena, Protégé, Neo4j for graph-based trust taxonomy storage and querying. Policy engines: Open Policy Agent (OPA), Cedar (AWS), Rego for policy evaluation. Compliance and regulatory intelligence: Thomson Reuters Regulatory Intelligence, LexisNexis Regulatory Compliance, Wolters Kluwer OneSumX. Standards frameworks: ISO 27001, SOC 2, HITRUST, NIST CSF, GDPR, HIPAA, EU AI Act, FedRAMP. Credential systems: W3C Verifiable Credentials, Decentralized Identifiers (DIDs), OpenBadges, mDL.

Installed Base

Regulatory compliance platforms (Thomson Reuters, LexisNexis, Wolters Kluwer) manage regulatory intelligence for millions of requirements across hundreds of jurisdictions. Policy engines (OPA, Cedar) process billions of policy decisions daily in cloud-native applications. Credential standards (W3C Verifiable Credentials, DIDs) define interoperable formats adopted by governments and enterprises. ISO, SOC 2, HITRUST, and FedRAMP frameworks collectively govern hundreds of thousands of enterprise compliance assessments annually. The UTM Runtime unifies these disparate compliance and credentialing systems into a single queryable trust substrate.

Total Addressable Value Enabled

The UTM Runtime is enabling infrastructure whose value is measured by the settlement it unlocks. Every PNX transaction that would be blocked by governance uncertainty, compliance ambiguity, or cross-domain trust incompatibility is enabled by the UTM's ability to resolve Trust Criteria programmatically. The global compliance industry—consulting, auditing, and regulatory technology—represents $50B+ annually in manual compliance labor that the UTM Runtime's automation capabilities can dramatically compress, while simultaneously enabling settlement that current compliance friction prevents.

Development Effort & AI Leverage

Prototype	Controlled Beta	GA Release	AI-Automatable
8–12 months	**14–20 months**	**24–36 months**	**55–70%**

AI can generate substantial portions of ontology definition, policy engine integration, credential lifecycle management, API development, and regulatory text parsing—particularly the natural-language-to-Trust-Criteria compilation, where LLMs excel at extracting structured requirements from legal and regulatory text. The primary human effort involves formal ontology design (ensuring consistency, completeness, and decidability of the five UTM ontologies), cross-jurisdiction regulatory mapping (understanding substantive legal differences between jurisdictions), and governance framework design determining how Trust Criteria evolve—areas requiring deep legal, regulatory, and ontological expertise.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

B.12 QPN Catalyst Application & Capture Module Specifications

This section provides detailed specifications for the QPN Catalyst application and its eight Catalyst Modules — the components that collectively implement the Quantum Privacy Catalyst Network's contribution capture, attribution, reputation, and administration capabilities.

Where B.11 (Foundational Enabling Services) describes the domain-agnostic infrastructure components that enable Resources to be published, settled, exchanged, and governed across the PNX, this section describes the Catalyst-specific components through which participants build and manage their Personal, Enterprise, and Accelerator Catalyst Networks. Section B.12.1 covers the QPN Catalyst application itself — the WebVector reference implementation that serves as the architectural hub. Sections B.12.2 through B.12.9 provide detailed component sheets for each of the eight Catalyst Modules, following the same specification format used in B.11: Description, Capabilities, QPN/PNX Implementation Role, Incremental QPN Value Add, Target Users, Platforms, Installed Base, Total Addressable Value Enabled, and Development Effort & AI Leverage.

B.12.1 QPN Catalyst Application: Reference Implementation Details

The QPN Catalyst application is the first deployed embodiment of the Accelerator Catalyst Layer architecture, implementing WebVector as the general-purpose capture hub. The following implementation details demonstrate enablement of the architectural patterns described in Sections 1–7 and Appendix B.11:

- **Contribution Type Taxonomy**: 19 types across 2 tiers (engagement: 9 types, major: 10 types) organized into 5 categories (relationship, commercial, trust, governance, infrastructure), plus 3 engagement signals (Meeting Requested, Introduction Requested, Follow-up Sent). Evidence required for major-tier types; optional but incentivized for engagement-tier. Evidence classified by strength (weak/medium/strong) based on nature.
- **Behavioral Activation System:** 10 levels (Observer through Founder, thresholds from 0 to 10,000 XP). 24 badges across 7 categories (getting started, volume, major, streak, special, recorder, reputation). Dual XP streams: contributor XP (earned by contributor) and recorder XP (5% of contributor XP, awarded only when recorder ≠ contributor). Evidence bonus: +25% of base XP. Streak multiplier: ×1.1 for 7+ consecutive days. Daily cap: 10 contributions.
- **Reputation Engine:** Pure computation module. Forward adjacency construction from ContributionLink records. DFS path finding for chain detection. 5-tier outcome confidence (highest/high/medium-high/medium/lower) based on objective priority gates and chain position. 7 reputation signals. 6 reputation badges (Chain Closer, Chain Catalyst, Objective Achiever, Cross Pollinator, Strong Evidence, Network Builder). Attribution readiness metric with expandable factor breakdown.
- **Proximity Engine:** 4-tier contributor-to-objective relevance: contributing (has linked contributions), nearby (90-day window, type/org match), program_active (active in program, no goal match), open (no connection). Gap templates with proximity-aware guidance. Deep links from objectives to filtered contribution views.
- **Goal Rules System:** linkedContributionCount variant with organization-scoped conditions (organizationIds, organizationMatch: any/all, distinctOrganizations). Goal progress computed at read time from contribution graph. Admin UI shows progress bars, matching/non-matching contribution split, and goal rule definitions.
- **Contribution Chain Graph Visualization:** Interactive directed graph with automatic layout. Shadow nodes for out-of-scope contributions preserving topology while anonymizing details. Edge types reduce to generic "linked" when shadow nodes are involved. Available on both contribution detail and objective detail views.

While email submission requires no account and no setup, participants who want greater control over their Catalyst experience can authenticate to the QPN Catalyst App. Authentication is entirely optional — email submission works indefinitely with zero setup — but unlocks several benefits:

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Notification and Alert Policies**: Configure how and when you receive notifications about activity in your contribution graphs — new submissions linked to your chains, milestone achievements, graph merges, or attribution events.
- **Multi-Factor Identity Binding**: Link multiple authentication coordinates — multiple email addresses, phone numbers, messaging contacts (WhatsApp, Signal, etc.), and verified identity information. This improves entity resolution accuracy (the system can match submissions from any linked identifier) and provides identity resilience (you retain access to your contribution history even if you lose control of any individual email address or account).
- **Contribution Graph Visibility**: View your contribution graphs, see how submissions are linked, track chain status, and monitor progress toward Activation Milestones.
- **Identity Resilience**: If you change jobs, lose an email address, or switch phone numbers, your linked identifiers ensure continuity across professional transitions.
- **Proxy Management**: Register and manage Authorized Catalyst Proxy Addresses, monitor forwarding activity, and view the contribution graphs routed through your proxies. Authentication at any time triggers entity resolution to link the authenticated identity to all prior submissions associated with the participant's email addresses and other identifiers.

B.12.2 WebVector (Contribution Capture & Administration Platform)

Description

The general-purpose web application that serves as the primary contributor interface and Accelerator Manager portal for the QPN Catalyst Network. WebVector is the architectural hub from which specialized Catalyst Modules (VoiceVector, DocVector, CommVector, MeetVector, MessageVector, AgentVector, CodeVector) extend — incorporating VoiceVector, DocVector, and CommVector (email intake) capabilities directly in its initial deployment while providing the administrative, analytical, and portfolio capabilities that no specialized Vector delivers independently. WebVector implements all five Signal Input Modes in their initial embodiments: Active Mode through four input methods (Voice, Paste, Upload, Manual), Directed Mode through email intake, and the foundational infrastructure for Ambient, Institutional, and Evangelized Modes as they activate in later phases. It also implements the behavioral activation system (XP, levels, badges, streaks), the reputation engine, proximity-based objective navigation, contribution chain graph visualization, program and objective management, and the three-ledger architecture (Contribution, Authorization, Settlement) that separates factual recording from governance enforcement and economic valuation. The QPN Catalyst application is the first WebVector embodiment.

Capabilities

- **Multi-modal contribution capture:** Four Active Mode input methods (Voice with real-time transcription, Paste for clipboard text, Upload for PDF/DOCX/TXT with SHA-256 hashing and auto-evidence, Manual for direct form entry) plus email intake for Directed Mode. All methods feed the same AI Evaluation Pipeline and produce identical Attribution Records. Entire recording flow completes in under 60 seconds.
- **AI-assisted field extraction:** LLM-powered extraction pipeline processes natural-language input to produce structured contribution records: contributor name, contribution type (classified against 19-type taxonomy), contact person, contact email, organization (matched against canonical directory with alias support), topic, and related-to connections. Engagement signal detection captures pre-milestone activity. Follow-up clarification questions resolve ambiguity when upgrade cues are detected. Domain glossary maps TLAs, abbreviations, and speech-recognition variations to canonical terms.
- **Behavioral activation system:** 10 levels (Observer through Founder), 24 badges across 7 categories (getting started, volume, major, streak, special, recorder, reputation), dual XP streams (contributor and recorder), evidence bonus (+25% of base XP), streak multiplier (×1.1 for 7+

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

consecutive days), daily cap (10 contributions). Persistent gamification bar on all contributor views surfaces level, impact score, XP progress, and active streak.

- **Reputation engine:** Pure computation module — DFS graph traversal across contribution chains, 5-tier outcome confidence classification (highest/high/medium-high/medium/lower), 7 reputation signals, 6 reputation badges (Chain Closer, Chain Catalyst, Objective Achiever, Cross Pollinator, Strong Evidence, Network Builder), attribution readiness metric, and network role classification. Operates on all contributions regardless of visibility settings.
- **Proximity-based objective navigation:** 4-tier proximity engine (contributing/nearby/program_active/open) with 90-day activity window, within-tier sorting by proximity level, "Your Position" activity blocks showing the contributor's relationship to each objective, gap templates with proximity-aware guidance, and deep links from objectives to filtered contribution views.
- **Contribution chain graph visualization:** Interactive directed graph with automatic layout on both contribution detail and objective detail views. Shadow nodes for out-of-scope contributions preserve topology while anonymizing details. Edge types reduce to generic "linked" when shadow nodes are involved.
- **Cryptographic receipting:** SHA-256 fingerprint from deterministic JSON serialization. Standalone receipt pages with tamper detection (verified/unverified/mismatch states). Downloadable PDF receipts with embedded QR codes. Share actions (email, copy link, copy details).
- **Program and objective management:** Full admin application with program management, objective management with goal rules (linkedContributionCount variant, organization-scoped conditions, distinctOrganizations), contribution-to-objective linking, contribution-to-contribution linking with typed edges (follow_up, outcome_of, enabled_by, duplicate_of), and analytics dashboard with system-wide reputation coverage metrics.
- **Contributor/admin dual-view architecture:** Separated Contributor App (personal view: Dashboard, Activity, Profile) and Admin App (aggregate view: Analytics, Programs, Objectives, Organizations) sharing a single codebase with scope switcher and role-based access control.
- **Contribution visibility model:** 4-tier contributor-controlled visibility (Confidential, Program, Accelerator, Network) with two-layer access model (role-based always-on plus contributor-chosen peer discovery scope). Evidence inherits parent contribution visibility or can be individually restricted.
- **Delegated attribution:** Any user can record contributions for themselves or on behalf of others. Contributor identified via voice input or explicit selection. Recorder XP (5% of contributor XP) awarded only when recorder ≠ contributor.

QPN/PNX Implementation Role

WebVector is the foundational application layer for the entire Accelerator Catalyst Network. Where VoiceVector, MeetVector, and MessageVector are specialized Catalyst Modules optimized for specific content domains and interaction patterns, WebVector provides the unified environment in which contributions are managed, analyzed, visualized, and administered regardless of which capture module originated them. It is the platform through which Accelerator Managers operate programs, link contributions to objectives, monitor reputation metrics, and oversee contribution graph formation. For contributors, it is the portfolio, reputation dashboard, and objective discovery surface that transforms raw contribution records into a professional identity artifact and a navigable view of network-building progress.

WebVector's architectural significance extends beyond its current capabilities. As the hub of the capture module architecture, it provides the web-based surface through which future capabilities — Ambient Mode agent proposals, Institutional Mode retrospective graph reviews, Evangelized Mode distribution tracking — are presented to contributors and administrators for review, confirmation, and governance. The agentic evolution (Phases 0–9) progressively transforms WebVector from an intelligent

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

recorder into a governed network coordination platform, with the agent proposing and the human approving through the same interface that currently handles Active Mode recording.

Incremental QPN Value Add

WebVector's incremental value is not in any single capture capability — VoiceVector, DocVector, and CommVector each handle their domains — but in the integration layer that makes the contribution graph coherent, navigable, and governable. Without WebVector, contributions captured by specialized modules would lack unified reputation scoring, proximity-based objective alignment, chain visualization, administrative linking, and the behavioral activation system that sustains contribution density during Phase 0. WebVector converts fragmented capture into a managed, attributed, governable contribution graph — which is the prerequisite for accurate retrospective settlement.

Target Users

All contributors and Accelerator Managers. Primary interface for Phase 0 contributors regardless of role. Sustained primary interface for Accelerator Managers, program administrators, and contributors who use multiple Catalyst Modules and need a unified view of their contribution portfolio, reputation, and objective alignment.

Platforms

Progressive web app (all modern browsers, mobile and desktop). API-first architecture enables future native mobile apps and integration with other AI surfaces (Catalyst Assistant browser extension, Claude Cowork Plugin, ChatGPT Connector, future MCP clients).

Development Effort & AI Leverage

Phase	Scope	Effort	AI-Automatable
Alpha / Phase 0	Multi-modal capture (Voice, Paste, Upload, Manual). AI Evaluation Pipeline. XP engine. Contribution Receipt. Proximity Objectives. Reputation Engine. Admin dual-view. Program/Objective management. Chain graph visualization.	**3–5 dev-mo**	**~70%**
Beta / Phase 1	Full "For Others" workflow with confirmation. Email intake (Directed Mode). Evidence strength classification. Goal rules with organization-scoped conditions. Shadow node graph privacy. Attribution readiness metric.	**3–5 dev-mo**	**~65%**
GA / Phase 2	API-first architecture extraction. Catalyst Assistant browser extension. Native mobile apps. EasyAccess IdP integration. Evangelized Mode attribution tracking. Agentic evolution Phases 0–2 (conversational context, chain nudging, Directed input expansion).	**6–10 dev-mo**	**~60%**

B.12.3 VoiceVector (Voice Narrative & Manual Contribution Capture App)

Description

A mobile and web application that enables contributors to record, classify, and attribute contribution events through natural-language voice narration, clipboard paste, or structured manual entry — without requiring installation of any plugin, browser extension, or enterprise integration. VoiceVector is the primary contribution interface for Phase 0 and for contributors whose work is primarily relational (meetings, introductions, advocacy, negotiations) rather than artifact-generating (code, documents, communications). It exposes the full the Three-Stage AI Evaluation Pipeline through a consumer-grade voice interface, producing Attribution Records indistinguishable in schema and provenance quality from records produced by any other capture module. VoiceVector also implements the "For Others" recording workflow, the XP engagement layer, the Contribution Receipt system, the Nearby Opportunities feed, and the contributor Impact Score dashboard.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Capabilities

- **Voice-to-attribution pipeline:** Real-time speech transcription → AI Evaluation Pipeline semantic classification → AI-extracted identity enrichment → pre-populated Review & Confirm screen → QPC-signed Attribution Record. Total time from "tap microphone" to confirmed record: under 60 seconds for a well-narrated contribution.
- **Three input modes:** Voice (microphone), Paste (clipboard import), Manual (structured form). All modes produce identical record schemas. Manual entry defaults to lower confidence; evidence attachment upgrades confidence at submission.
- **Delegated Attribution:** records can be attributed to any named contributor as Attribution Recipient, subject to PENDING_CONTRIBUTOR_CONFIRMATION workflow (see §9.2)
- **XP engagement layer:** Base XP by contribution type, Evidence Bonus (~25% of base for attached evidence), Streak Bonus (% multiplier for daily consecutive contributions). Daily cap (default 10 records) prevents gaming. Streak counter displayed prominently.
- **Contributor level progression:** Named levels earned through XP accumulation. Level titles aligned with contribution category patterns (Advocate, Connector, Catalyst track for relationship-intensive contributors; Builder, Architect track for technical contributors).
- **Contribution Receipt:** AI-generated title, Receipt number (short hash), XP breakdown, Nearby Objectives panel. Exportable as PDF, email, link, or structured text.
- **Nearby Opportunities feed:** Personalized program objective surface generated from the contributor's graph proximity and objective progress gaps. Labels: Contributing / Nearby / Available.
- **Impact Score dashboard:** Composite quality metric (Evidence Attached / In Outcome Chains / Linked to Objectives / Major-Tier Contributions) displayed in contributor Profile.
- **My Network analytics:** Organizations count, People Connected count, Programs Active count, Contributions Made count, Recorded for Others count. Contribution type breakdown (Introduction / Meeting / Amplification / Referral / Strategic Partnering MOU Signed).
- **Admin View toggle:** Dual-mode interface: Contributor View (personal dashboard) and Admin View (Programs, Accelerators, Organizations, Analytics, Objective Linking). Role-based access; Managers switch views without logging out.

QPN/PNX Implementation Role

VoiceVector is the bootstrap mechanism for the entire Catalyst Network and is a primary active contribution interface for Phase 0. Along with MessageVector, it requires zero enterprise integration and zero plugin installation — any contributor can begin capturing attribution records from a phone or browser within minutes of onboarding. Where VoiceVector excels is in active, narrated capture: a Managing Director at a health system, a government policy advisor, or a venture capital partner can open the web app on their phone, say "I introduced [name] at [org] to the Lokahi team today, here is their email," and generate a cryptographically signed, AI-classified attribution record in under 60 seconds. MessageVector handles the passive inbound channel — documents, replies, and signed agreements that arrive without any contributor action. Together they ensure that no contribution event is missed, whether the contributor initiates it or the counterparty does. This is "If you helped build it, you should own a piece of it" operating at both ends of every interaction.

Target Users

All contributors during Phase 0. Sustained primary interface for relationship-intensive contributors (executives, business development professionals, ecosystem orchestrators, government relations leads, venture investors, strategy consultants) whose highest-value contributions are meetings, introductions, and advocacy activities that do not generate digital artifacts automatically captured by other modules.

Platforms

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Progressive web app (iOS Safari, Android Chrome, desktop browsers). Native iOS and Android apps in Phase 2. Desktop keyboard shortcut (Press R) for rapid contribution entry during active working sessions.

Development Effort & AI Leverage

Phase	Scope	Effort	AI-Automatable
Alpha / Phase 0	Voice + Paste + Manual input. AI Evaluation Pipeline classification. Basic .qpn archive storage. XP engine. Contribution Receipt. Nearby Opportunities feed (rule-based).	**1–2 dev-mo**	**~75%**
Beta / Phase 1	Full "For Others" workflow with confirmation. Impact Score dashboard. Admin View with Programs and Objective Linking. Streak mechanics and daily cap. Graph proximity-based Nearby Opportunities.	**2–4 dev-mo**	**~65%**
GA / Phase 2	Native iOS/Android apps. Real-time CCP integration (auto-populate known contacts). Cross-session cascade detection. Retrospective bulk import from archive.	**4–6 dev-mo**	**~60%**

B.12.4 CodeVector (DevOps & Engineering Attribution Engine)

Description

A privacy-preserving attribution engine that captures code commits, pull requests, repository contributions, and engineering artifacts through developer toolchain integration — producing cryptographically signed attribution records that verify contributions occurred, link them to the contributor's QPC, and preserve chain relationships to upstream and downstream engineering activity, without extracting or transmitting proprietary source code. CodeVector operates at the toolchain layer through Git hooks, CI/CD pipeline plugins, and IDE extensions, making attribution capture invisible within the developer's existing workflow. For artifact-generating technical contributors, every commit, merge, deployment, and infrastructure contribution becomes a settlement-eligible attribution record at zero incremental effort.

Capabilities

- **Commit-level hash attestation:** SHA-256 hash of staged diff content signed with the contributor's QPC key at commit time. The hash verifies that the contribution occurred and captures its scope without exposing the underlying code. Optionally injected into the commit trailer as an X-QPN-Attribution header for provenance tracing within the repository history.
- **Pull request and merge attribution:** Captures pull request creation, review activity, and merge events as distinct contribution records. Review contributions (code review, architecture feedback, security assessment) are attributed separately from authorship contributions, enabling attribution for the review and governance work that is often more valuable than the code itself.
- **CI/CD pipeline completion tracking:** Automated deployment confirmation records generated when CI/CD pipelines complete successfully, upgrading contribution status from CODE_COMMITTED to CODE_DEPLOYED. Deployment fingerprints capture infrastructure state at deployment time, linking code contributions to production outcomes.
- **AI Evaluation Pipeline classification:** The pipeline classifies each contribution by type (new feature, bug fix, infrastructure, documentation, security hardening, test coverage, adapter/connector development) and detects chain relationships to upstream requirements (issues, specifications, bounties) and downstream deployments. Cascade indicators identify contributions that enabled or unblocked subsequent work by other contributors.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Software supply chain attestation:** Generates attestations conforming to SLSA and in-toto frameworks, linking build provenance to software supply chain governance. Automated SBOM (Software Bill of Materials) generation with PNX Resource linkage enables downstream consumers to verify the provenance and governance of every component.
- **Infrastructure-as-code reuse attribution:** Shared Terraform, Helm, CloudFormation, and other infrastructure-as-code modules that are reused across Exchange Networks generate settlement-eligible reuse events, enabling the original contributors to earn Exchange Tokens proportional to downstream deployment.
- **Repository and file path privacy:** Repository names, branch names, and file paths are redacted to opaque tokens in the attribution record. Only classification metadata (contribution type, language, complexity estimate, chain indicators) is stored, ensuring full compatibility with enterprise DLP policies.

QPN/PNX Implementation Role

CodeVector is the primary capture module for the Race to Deploy (Section 3.3). The Foundational Enabling Services, platform adapters, connectors, and infrastructure integrations described in B.11 and B.12 all flow through developer toolchains — and CodeVector ensures that every line of code, every deployment, and every infrastructure contribution can be attributed to the individuals and teams who built it. The first team to publish a high-quality connector for any given platform captures the Quantum Privacy Rewards for every downstream settlement event that connector enables, regardless of whose platform it targets. CodeVector provides the attribution infrastructure that makes this competitive dynamic precise and verifiable.

CodeVector also serves as the foundation for open-source economic sustainability within the QPN ecosystem. Open-source contributors who build reusable components — adapters, libraries, governance frameworks, trust taxonomy implementations — earn Exchange Tokens whenever those components are deployed, reused, or incorporated into Resource Derivatives across Exchange Networks. This transforms open-source contribution from a reputation-only activity into a settlement-linked economic participation, directly addressing the sustainability challenge that limits open-source ecosystem development.

Incremental QPN Value Add

- **Attribution completeness for technical contributors** — developers, engineers, and infrastructure teams whose work is entirely artifact-generating receive automatic, zero-effort attribution for every commit, merge, and deployment without changing their workflow.
- **Cross-module cascade chains** — code contributions that implement commitments captured by MeetVector (COMMITMENT_STATED → CODE_COMMITTED → CODE_DEPLOYED), fulfill bounties posted through the coordination marketplace, or execute partnerships captured by DocVector create multi-module cascade chains with the highest attribution confidence scores.
- **Reusable infrastructure settlement** — shared components, adapters, and infrastructure-as-code modules generate ongoing Exchange Token settlement proportional to downstream reuse, creating a perpetual revenue stream for foundational technical contributions.
- **Software supply chain governance** — SLSA-conformant attestations and automated SBOM generation provide the provenance and governance evidence required for Trust Block verification in regulated deployment environments.
- **Competitive adapter development incentive** — the Race to Deploy dynamics (Section 3.3) create a competitive land-grab where engineering teams race to build and publish adapters for every major platform, with CodeVector providing the attribution infrastructure that ensures the winning team captures the Quantum Privacy Rewards.

Target Users

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Software engineers, DevOps engineers, platform engineers, site reliability engineers, infrastructure architects, open-source maintainers, security engineers, and technical contributors whose primary work product is code, configuration, or infrastructure artifacts.

Platforms

Git-based version control: GitHub, GitLab, Bitbucket, and any Git-compatible system. IDEs: VS Code, JetBrains (IntelliJ, PyCharm, WebStorm), Xcode. CI/CD: GitHub Actions, GitLab CI/CD, Jenkins, CircleCI, Azure DevOps Pipelines, AWS CodePipeline, Buildkite. Container and infrastructure: Docker, Kubernetes, Terraform, Helm, CloudFormation.

Installed Base

GitHub serves over 100 million developers with over 300 million repositories. GitLab has over 30 million registered users. VS Code is the most widely used IDE globally with over 70% market share among professional developers. Jenkins remains deployed in hundreds of thousands of enterprise environments. The combined developer toolchain ecosystem processes billions of commits, builds, and deployments annually. Virtually every software-producing organization in the world uses at least one of these platforms.

Total Addressable Value Enabled

The global software economy exceeds $5 trillion annually, with software engineering labor representing the largest single cost category. If even a small share of this activity—on the order of 5%—occurred within PNX-connected Exchange Networks, it would represent over $250 billion in engineering effort associated with traceable, settlement-eligible contributions. Because software components are reused across many environments, the economic impact compounds: a single adapter, library, or infrastructure module deployed across hundreds of Exchange Networks generates settlement proportional to the downstream activity it enables, not merely the initial development effort. CodeVector's alignment with emerging software supply-chain governance standards such as SLSA and SBOM provides a natural compliance-driven pathway for adoption within regulated industries.

Development Effort & AI Leverage

Phase	Scope	Effort	AI-Automatable
Alpha / Phase 0	Git commit/push hook with SHA-256 hashing. QPC key signing. Local .qpn archive storage. Basic AI Evaluation Pipeline classification (contribution type, language, complexity). X-QPN-Attribution commit trailer injection.	**1–2 dev-mo**	**~80%**
Beta / Phase 1	Pull request and merge event capture. CI/CD pipeline completion tracking (GitHub Actions, GitLab CI). CODE_COMMITTED → CODE_DEPLOYED status upgrade. Chain relationship detection to upstream issues and downstream deployments. Repository/file path redaction to opaque tokens.	**2–4 dev-mo**	**~70%**
GA / Phase 2	Full CI/CD platform coverage. SLSA-conformant supply chain attestation. SBOM generation with PNX Resource linkage. Infrastructure-as-code reuse attribution. Cross-module cascade linkage (MeetVector commitments, DocVector agreements, bounty fulfillment). IDE plugin distribution (VS Code, JetBrains).	**4–6 dev-mo**	**~65%**

The core hashing and signing logic is straightforward and highly automatable. Git hook patterns are well-documented and AI tools excel at generating them. The primary human-intensive work involves CI/CD platform normalization across providers, SLSA compliance verification, and cross-module cascade linkage logic. Pull request review attribution requires nuanced understanding of code review workflows that benefits from human design input.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

B.12.5 DocVector (Legal, Governance & Formal Documentation Attribution Engine)

Description

A privacy-preserving attribution engine that captures signed agreements, authored documents, governance frameworks, compliance artifacts, and other formal work products through document upload with cryptographic binding, e-signature platform integration, and native Privacy Network-enabled document signing. DocVector produces cryptographically signed attribution records that verify a formal document was created, executed, or delivered — linking it to the contributor's QPC and preserving chain relationships to the introductions, meetings, and negotiations that preceded it — without transmitting document content outside the contributor's security perimeter. DocVector operates through three complementary pathways: direct document upload through WebVector (immediate, no integration required), native e-signature platform integration (automated capture with lifecycle tracking from envelope creation through execution), and native Privacy Network signing (QPC-based cryptographic signing through any QPN Catalyst interface at zero cost, without requiring any third-party platform).

Capabilities

- **Document-level hash attestation:** SHA-256 hash of the uploaded or signed document binary, signed with the contributor's QPC key at the moment of capture. The hash provides tamper-evident proof that a specific document existed in a specific state at a specific time, without exposing its content.
- **E-signature lifecycle tracking:** For natively integrated platforms, DocVector monitors the full document lifecycle — envelope creation, signature request, counterparty review, signature completion — upgrading contribution status from DOCUMENT_SENT to DOCUMENT_SIGNED upon webhook confirmation of completed execution. An opaque Catalyst ID is injected as a hidden EnvelopeCustomField where the platform supports it, enabling automated matching between the e-signature event and the attribution record.
- **Native Privacy Network-enabled document signing:** Contributors and counterparties can verify authorship, review, approval, or execution of any document directly through their Quantum Privacy Cells — without requiring a third-party e-signature service. The signer's QPC key cryptographically signs the document hash, producing a verifiable attestation that a specific individual with a specific QPC identity attested to the document at a specific time. Multiple signatories sign sequentially or in parallel, with each signature recorded as a Trust Block-wrapped Verifiable Credential linked to the signer's QPC. This native signing capability is free, unlimited, and produces attribution records with stronger provenance than third-party e-signature platforms — because the cryptographic identity is anchored in the QPN's Proof of Trust infrastructure rather than in a vendor-specific identity verification system. The operational costs of enterprise-grade document signing — authentication, identity proofing, secure storage, audit trails, tamper detection, and delivery notifications — are available as by-products of the Personal Privacy Network and QPN Catalyst infrastructure that already operates for contribution capture, governance, and settlement, enabling native signing to be delivered at negligible marginal cost. For contributors in jurisdictions where e-signature services are unavailable, prohibitively expensive, or legally insufficient, native QPC signing provides a universally accessible alternative. For high-volume governance work — where trust framework authors, compliance architects, and Trust Authority specifiers may produce dozens of signed specifications — the elimination of per-envelope fees removes a structural barrier to contribution. Native signing integrates with the same AI Evaluation Pipeline classification, evidence auto-attachment, and cross-module chain linkage as e-signature platform integration, ensuring identical attribution quality regardless of which signing method is used.
- **AI-assisted document classification:** Server-side text extraction and LLM-assisted field parsing identify the contribution type (partnership agreement, MOU, LOI, teaming agreement, licensing agreement, data sharing agreement, governance framework, trust authority specification, compliance certification, regulatory filing), counterparties, commercial terms referenced, and

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

chain relationships to prior contributions. The AI Evaluation Pipeline's causal-enablement logic determines whether the document represents a new Institutional Activation Milestone or an advancement of an existing cascade chain.

- **Auto-evidence attachment with strength classification:** Uploaded documents are automatically attached as evidence to the attribution record with SHA-256 cryptographic binding. Evidence strength is rule-based: TXT → weak, PDF/DOCX → medium, signed agreements with counterparty identification → strong. The auto-attachment immediately qualifies the contribution for the Evidence Bonus in the behavioral activation system.
- **Cross-module chain linkage:** DocVector records are automatically linked to upstream contributions that led to the documented outcome — an introduction captured by CommVector or VoiceVector, a meeting captured by MeetVector, a verbal commitment tracked as COMMITMENT_STATED — creating a complete provenance chain from first contact through formal execution. This cross-module linkage produces the highest-confidence cascade chains in the attribution system.
- **Retrospective document archaeology:** Bulk processing of historical document repositories — contract management systems, SharePoint libraries, Google Drive folders, local file archives — to identify and classify previously unattributed formal work products. Particularly valuable when an enterprise activates Institutional Mode and authorizes retrospective processing of its document management infrastructure.
- **Multi-format support:** Processes PDF, DOCX, DOC, TXT, and image-based documents (via OCR). Scanned physical documents, faxed agreements, and photographed signatures are processed identically to native digital documents, ensuring attribution completeness across all document formats encountered in practice.

QPN/PNX Implementation Role

DocVector captures the documentary evidence of institutional commitments — the signed agreements, MOUs, partnership frameworks, and governance specifications that represent the most heavily weighted Institutional Activation Milestones in the Quantum Privacy Rewards framework.

Where CommVector captures the outreach that initiates a relationship and MeetVector captures the meetings where commitments are made, DocVector captures the formal execution that converts verbal intent into binding obligation.

A complete cascade chain — introduction (CommVector/VoiceVector) → meeting (MeetVector) → verbal commitment (MeetVector COMMITMENT_STATED) → signed agreement (DocVector DOCUMENT_SIGNED) — is the gold standard of attribution evidence, and DocVector provides the terminal node that confirms the chain produced a real institutional outcome.

The native Privacy Network-enabled signing capability extends this to any participant anywhere in the world at zero cost — eliminating dependence on commercial e-signature platforms as a gating requirement for formal document attribution and enabling the grassroots cascade to produce fully attributed institutional milestones without enterprise procurement cycles.

DocVector is also the primary capture module for governance contributions — trust framework authorship, trust taxonomy specifications, compliance architecture documents, and Trust Authority certification materials. These contributions carry premium Quantum Privacy Rewards under the Governance Premiums because they embed the governance DNA that shapes the behavior of every downstream Resource Derivative. DocVector ensures that the individuals who author governance frameworks receive durable, verifiable attribution for work that compounds across the entire ecosystem.

Incremental QPN Value Add

- **Attribution completeness for institutional milestones** — the most heavily weighted contribution types (signed partnerships, executed MOUs, governance frameworks) are captured with the highest

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

evidence strength, ensuring that the contributors who closed the most valuable deals receive proportionally accurate Quantum Privacy Rewards.

- **Cross-module cascade completion** — DocVector records serve as the terminal confirmation node for cascade chains initiated by other modules, converting multi-step attribution sequences from "probably led to an outcome" to "verifiably produced this signed agreement."
- **Governance DNA attribution** — trust framework authors, compliance architects, and Trust Authority specifiers receive permanent, evidence-backed attribution for governance contributions that compound through every generation of Resource Derivatives governed by their frameworks.
- **Zero-cost universal document signing** — native QPC-based signing eliminates per-envelope fees and third-party platform dependence, enabling grassroots contributors, small organizations, and international participants to produce fully attributed signed documents with cryptographic provenance stronger than commercial e-signature services — delivered at negligible marginal cost because the underlying infrastructure (authentication, identity proofing, secure storage, audit trails, tamper detection, delivery notifications) already operates for contribution capture, governance, and settlement.
- **Retrospective value recovery** — enterprises activating Institutional Mode can process years of document archives to surface formal agreements, governance frameworks, and compliance certifications that were never attributed at the time of execution, recovering attribution credit for historical ecosystem-building activity.
- **E-signature platform competitive incentive** — platforms that integrate DocVector natively (providing automated lifecycle tracking and end-to-end provenance) give their enterprise customers higher attribution confidence scores, creating a market differentiator that accelerates native integration across the e-signature ecosystem.

Target Users

Legal professionals, partnership managers, business development executives, governance specialists, compliance officers, trust framework authors, enterprise counsel, contract managers, and any contributor whose ecosystem-building work produces formal documentation — signed agreements, governance frameworks, regulatory filings, or compliance certifications.

Platforms

E-signature platforms: DocuSign, Adobe Acrobat Sign, Dropbox Sign, PandaDoc, HelloSign. Document management: SharePoint, Google Drive, Box, Dropbox Business, enterprise contract management systems.

Native Privacy Network signing: QPC-based cryptographic signing through any QPN Catalyst interface (web, mobile, API) — no third-party platform required. Direct upload: any document accessible to the contributor through WebVector's Upload input method (PDF, DOCX, DOC, TXT, images).

Installed Base

DocuSign serves over 1.5 million customers and processes hundreds of millions of envelopes annually. Adobe Sign, Dropbox Sign, PandaDoc, and HelloSign collectively serve millions of additional users. Enterprise document management platforms (SharePoint, Google Drive, Box) are deployed in virtually every Global 2000 company.

Native Privacy Network signing extends the addressable base beyond commercial e-signature customers to any individual or organization with a QPC — including grassroots contributors, small businesses, international participants in jurisdictions where commercial e-signature services are unavailable or legally insufficient, and high-volume governance contributors for whom per-envelope fees represent a structural barrier. The total addressable contributor base includes every professional who produces, signs, or manages formal business documents — spanning legal, commercial, governance, and compliance functions across all industries.

Total Addressable Value Enabled

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Global contract and agreement volume exceeds $100 trillion annually across all commercial sectors. Governance frameworks, trust specifications, and compliance certifications represent an additional multi-trillion-dollar category of institutional value creation that is currently unattributed. Even linking 1% of formally executed agreements to PNX settlement chains would represent over $1 trillion in attributable value. The value amplifies through governance DNA inheritance: a trust framework authored once and embedded in Trust Blocks across thousands of Resource Derivatives generates settlement proportional to every downstream transaction governed by that framework, not just the initial authorship effort. Native Privacy Network signing further amplifies the addressable value by removing the cost barrier that currently prevents high-volume, low-value-per-document signing from being economically viable — enabling categories of formal attribution (governance framework endorsements, Trust Authority certifications, multi-party resource pool agreements, community Accelerator formation documents) that would never justify commercial e-signature fees individually but collectively represent significant settlement value at ecosystem scale.

Development Effort & AI Leverage

Phase	Scope	Effort	AI-Automatable
Alpha / Phase 0	Document upload through WebVector with SHA-256 hashing and auto-evidence attachment. AI Evaluation Pipeline classification (contribution type, counterparty extraction, chain relationship detection). Rule-based evidence strength classification.	**1–2 dev-mo**	**~75%**
Beta / Phase 1	DocuSign native integration (envelope creation webhook, EnvelopeCustomField injection, EnvelopeCompleted lifecycle tracking, DOCUMENT_SENT → DOCUMENT_SIGNED status upgrade). Native Privacy Network signing (QPC key document hash signing, multi-signatory sequential and parallel flows, Trust Block-wrapped signature VCs). Cross-module chain linkage to CommVector and MeetVector records. Retrospective document archaeology for bulk archive processing. Multi-format support including OCR for scanned documents.	**3–6 dev-mo**	**~65%**
GA / Phase 2	Full e-signature platform coverage (Adobe Sign, Dropbox Sign, PandaDoc, HelloSign). Enterprise document management integration (SharePoint, Google Drive, Box). Institutional Mode bulk processing for enterprise document repositories. Governance framework classification with Trust Block criteria mapping. Cross-Accelerator governance contribution attribution.	**4–7 dev-mo**	**~60%**

The core document hashing, upload processing, and AI classification logic reuses the existing AI Evaluation Pipeline with document-specific extraction prompts. E-signature platform API integration follows well-documented webhook patterns that are highly amenable to AI-assisted development. Native Privacy Network signing leverages the QPC cryptographic infrastructure already defined in the architecture — the core signing operation is straightforward, though the multi-party signing flow (sequential/parallel, partial completion states, signature status tracking) requires careful workflow design. The operational costs that make commercial e-signature services expensive (identity verification, authentication, secure storage, audit trails, tamper detection, delivery notifications) are already borne by the Personal Privacy Network and QPN Catalyst infrastructure, making the marginal cost of native signing negligible. The primary human-intensive work involves multi-platform lifecycle normalization (each e-signature vendor has different event schemas and completion semantics), governance document classification taxonomy design, and retrospective archaeology pipeline optimization for large enterprise archives.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

B.12.6 AgentVector (AI-Assisted Research & Agentic Workflow Attribution Engine)

Description

A privacy-preserving attribution engine that captures AI-assisted research sessions, agentic workflow outputs, and human-AI collaborative work products — producing cryptographically signed attribution records that verify a contributor guided AI tools to specific, verifiable outcomes without exposing prompts, intermediate reasoning, or model internals. AgentVector operates across any AI platform accessible via API, MCP, session export, or browser extension, generating Proof of Orchestration attestations that attribute the human's direction, judgment, and orchestration rather than the AI's mechanical execution. As AI-assisted development accelerates across the ecosystem, AgentVector captures the growing category of contributions where the contributor's primary value lies in knowing what to ask, how to evaluate the output, and when the result is good enough to act on.

Capabilities

- **Session-level hash attestation:** SHA-256 hash of interaction logs (prompt metadata and completion metadata) signed with the contributor's QPC key at session end or contributor-initiated checkpoint. The hash verifies that a specific human-AI interaction occurred and produced a specific outcome, without exposing the prompts, completions, or model internals that constituted the session.
- **Proof of Orchestration generation:** A structured attestation verifying that the contributor directed the AI to produce a specific, verifiable outcome — algorithm design, architecture specification, compliance mapping, integration documentation, research analysis, strategy development, trust taxonomy authorship, policy drafting, or data analysis. The Proof of Orchestration captures the nature and classification of the outcome without revealing the reasoning chain that produced it, establishing the contributor's intellectual contribution independently of the AI's mechanical role.
- **AI Evaluation Pipeline classification:** The pipeline classifies each contribution against the canonical taxonomy, records semantic contribution classification and cascade indicators, and extracts identity attributes for any persons or organizations referenced in the session output. Classification distinguishes between contribution types (new research finding, architecture specification, compliance framework, strategy document, model evaluation, trust taxonomy, policy draft) and assigns confidence scores reflecting the verifiability and specificity of the outcome.
- **Cross-session cascade detection:** For multi-session research workflows that extend across days or weeks, the Contributor Context Profile (CCP) links related sessions into a unified contribution chain. A research effort that begins with an exploratory session in Week 1, produces a draft framework in Week 3, and yields a completed governance specification in Week 6 is attributed as a single cascade chain with progressively strengthening confidence scores — not as three unrelated contributions.
- **Multi-platform capture:** Supports any AI platform through four integration modes: QPN Catalyst Native (session output pasted or uploaded through WebVector), SuperPrompt (EP3 Contribution Context loaded into the AI session with structured delta exported at session end), Browser Extension (Catalyst Assistant captures session context automatically), and API-Level (server-side integration for enterprise AI deployments). All modes produce identical Attribution Records.
- **Ambient Mode agent detection:** In later agentic evolution phases (Phases 5–6), AgentVector monitors authorized AI platforms with per-contributor opt-in, detecting contribution-worthy activity — research findings that advance program objectives, analysis outputs that resolve open questions, model evaluations that inform architecture decisions — and proposing attribution records for human confirmation. All Ambient Mode proposals require explicit human approval before any record is created, regardless of consequence level, because ambient signals lack human intent.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Collaborative AI attribution:** When multiple contributors collaborate through shared AI sessions, AgentVector attributes contributions to each participant based on their orchestration role — who framed the problem, who directed the analysis, who evaluated and refined the output, who applied the result. Collaborative attribution is recorded through the standard Delegated Attribution workflow, with each contributor's role and contribution boundary explicitly captured.
- **Model and tool provenance tracking:** AgentVector records which AI models and tools were used in each session (model identifier, version, capabilities invoked) without exposing the session content. This provenance metadata feeds into the Global Graph Assembly Engine's attribution chain reconstruction, enabling the system to distinguish between contributions that required sophisticated AI orchestration (multi-model workflows, custom tool chains, domain-specific prompting) and simpler interactions.

QPN/PNX Implementation Role

AgentVector addresses the fastest-growing category of professional contribution: AI-assisted knowledge work. As AI tools become integral to research, analysis, strategy, governance, compliance, and technical development, an increasing fraction of the most valuable ecosystem-building activity occurs through human-AI collaboration rather than purely human effort. Without AgentVector, a contributor who spends hours directing Claude to produce a comprehensive trust taxonomy, guiding Gemini through a multi-source regulatory analysis, or orchestrating a multi-model workflow to evaluate architecture alternatives generates no attributable record of that work — even though their direction, judgment, and domain expertise were the essential inputs that produced the outcome.

AgentVector is particularly critical for the contribution categories that will dominate later phases of ecosystem development: Trust Framework Authored, Safety Assessment Completed, Technical Validation, and Infrastructure Development. These categories increasingly involve AI-assisted workflows where the human's contribution is orchestration and judgment rather than manual execution. AgentVector ensures that the shift toward AI-assisted work does not erode attribution accuracy — the humans who direct AI tools toward ecosystem-building outcomes receive the same quality of attribution as contributors who produce artifacts manually.

AgentVector also serves as the foundation for the agentic economy within the QPN — where AI agents operating under QPC governance contribute to Exchange Networks, Resource Pools, and settlement flows. As agents become more autonomous (Phases 6–9 of the agentic evolution), AgentVector's Proof of Orchestration model extends to attribute the human governance decisions that authorize and direct agent activity, ensuring that economic value generated by agents flows to the humans whose judgment and governance made that activity possible.

Incremental QPN Value Add

- **Attribution completeness for AI-assisted contributions** — researchers, analysts, architects, governance specialists, and strategists whose most valuable work occurs through AI collaboration receive verifiable, settlement-eligible attribution for orchestration and judgment that would otherwise be invisible.
- **Cross-session cascade attribution** — multi-week research efforts, iterative framework development, and long-running analysis projects are attributed as unified cascade chains rather than fragmented individual sessions, producing more accurate Quantum Privacy Rewards for sustained intellectual contributions.
- **Proof of Orchestration as professional credential** — AgentVector records become a verifiable record of a contributor's ability to direct AI tools toward high-value outcomes, strengthening their Quantum Reputation and creating a portable professional credential for AI-era knowledge work.
- **Foundation for agentic economy attribution** — as AI agents become more autonomous within the QPN ecosystem, AgentVector provides the attribution infrastructure that links agent-generated economic value back to the human governance and orchestration decisions that enabled it.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Multi-model workflow attribution** — contributors who orchestrate complex workflows spanning multiple AI platforms, custom tool chains, and domain-specific models receive attribution reflecting the sophistication of their orchestration, not just the outputs produced.
- **AI platform competitive incentive** — AI platforms that integrate AgentVector natively (providing automatic session capture and Proof of Orchestration generation) give their users higher attribution confidence scores, creating a market differentiator that accelerates native integration across the AI platform ecosystem.

Target Users

AI researchers, data scientists, strategy consultants, governance specialists, compliance architects, trust framework authors, technical architects, policy analysts, and any knowledge worker whose primary contribution involves directing AI tools toward specific, verifiable outcomes.

Also: enterprise AI teams operating shared model deployments where multiple contributors collaborate through common AI infrastructure, and open-source AI contributors whose model fine-tuning, evaluation, and documentation work occurs primarily through AI-assisted workflows.

Platforms

AI platforms: Claude (Anthropic), ChatGPT (OpenAI), Gemini (Google), Grok (xAI), GitHub Copilot, Microsoft Copilot, Amazon Q, and any AI tool accessible via API or session export. Development environments: Claude Code, OpenAI Codex, Cursor, Replit AI, and AI-integrated IDEs. Agent orchestration frameworks: LangChain, CrewAI, AutoGen, and emerging multi-agent platforms operating within QPC-bounded Privacy Domains. Browser extension: Catalyst Assistant for automatic session capture across web-based AI platforms. MCP integration: Claude Cowork Plugin, ChatGPT Connector, and future MCP clients.

Installed Base

ChatGPT has over 200 million weekly active users. Claude, Gemini, and Copilot collectively serve tens of millions of additional users. GitHub Copilot is used by over 1.8 million paid subscribers and millions more through free tiers. The combined AI platform user base exceeds 500 million and is growing rapidly. Enterprise AI deployments span virtually every Global 2000 company. The total addressable contributor base for AgentVector is the entire population of professionals who use AI tools in their work — a population that is expanding by hundreds of millions annually as AI becomes integral to every knowledge-work domain.

Total Addressable Value Enabled

AI-assisted knowledge work is projected to contribute over $10 trillion annually to the global economy by 2030, with AI tools augmenting or automating significant portions of research, analysis, strategy, compliance, and technical development across every sector. Even attributing 5% of AI-assisted professional output to PNX-connected Exchange Networks would represent over $500 billion in traceable, settlement-eligible value. The value amplifies as AI orchestration becomes more sophisticated: a contributor who directs a multi-model workflow to produce a comprehensive trust taxonomy that is subsequently adopted across dozens of Exchange Networks generates settlement proportional to every downstream transaction governed by that taxonomy — not just the initial orchestration effort. AgentVector ensures that this compounding attribution flows to the human whose judgment produced the outcome.

Development Effort & AI Leverage

Phase	Scope	Effort	AI-Automatable
Alpha / Phase 0	Session output capture through WebVector (Paste and Upload input methods). AI Evaluation Pipeline classification of AI session outputs. Proof of Orchestration generation from structured session metadata. QPC key signing and .qpn archive storage. Basic cross-session cascade detection through CCP.	**1–2 dev-mo**	**~75%**

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Beta / Phase 1	SuperPrompt integration with structured delta export for Claude, ChatGPT, Gemini, and Grok. Catalyst Assistant browser extension for automatic session capture. Collaborative AI attribution with Delegated Attribution workflow. Model and tool provenance tracking. Cross-session cascade detection with multi-week chain linking.	**3–5 dev-mo**	**~70%**
GA / Phase 2	API-Level integration for enterprise AI deployments. Ambient Mode agent detection (Phases 5–6 agentic evolution) with mandatory human approval. Multi-model workflow attribution across orchestration frameworks (LangChain, CrewAI, AutoGen). MCP integration (Claude Cowork Plugin, ChatGPT Connector). Native platform integration for automatic Proof of Orchestration generation.	**4–7 dev-mo**	**~65%**

The core classification and attribution logic reuses the existing AI Evaluation Pipeline — AI session outputs are processed as text inputs through the same semantic classification engine used for all other Catalyst Modules. Proof of Orchestration generation is a structured metadata operation that is highly automatable. The primary human-intensive work involves cross-platform session capture normalization (each AI platform exposes session data differently), collaborative attribution workflow design for multi-contributor sessions, and Ambient Mode detection threshold calibration to minimize false-positive contribution proposals while capturing genuine orchestration activity. The browser extension and MCP integration require platform-specific engineering but follow well-documented extension APIs.

B.12.7 CommVector (Outreach, Advocacy & Relationship Attribution Engine)

Description

A privacy-preserving attribution engine that captures outreach, advocacy, and relationship-building activity across email, messaging, and professional networking channels — with verified engagement tracking that distinguishes between mere activity (sending a message) and demonstrated impact (receiving a response, advancing a relationship, triggering a downstream commitment).

CommVector operates across Active Mode (contributors record interactions through WebVector), Directed Mode (contributors CC the Catalyst agent on outgoing emails, triggering automatic extraction and attribution), and Evangelized Mode (attribution-tracked distribution of awareness and participation content through any channel). CommVector produces the outbound half of the attribution loop — the introductions, follow-ups, presentations, and advocacy that initiate cascade chains — while MessageVector (B.12.9) captures the inbound responses and documents that confirm those chains produced results.

Capabilities

- **Real-time verified engagement loop:** For outbound communications, CommVector generates a hash from the message body text, recipient domain, and ISO 8601 timestamp — H(Body_Text + Recipient_Domain + ISO8601_Timestamp) — and captures the Message-ID for downstream matching. The Listener Agent polls the sending platform's API for In-Reply-To or thread_ts references matching the captured Message-ID. Upon valid reply detection, record status upgrades from SENT to VERIFIED_ENGAGEMENT; reply metadata (timestamp, thread depth, reply domain) is appended; and the cascade indicator is updated based on reply content classification. This cryptographic engagement verification transforms "I sent an email" into "I sent an email and received a verified response" — a materially stronger attribution claim.
- **Multi-channel outreach capture:** Supports email (Gmail, Outlook, any SMTP-accessible client), messaging platforms (Slack, LinkedIn, WhatsApp, Signal, Telegram, iMessage, SMS), and professional networking channels. In Active Mode, contributors record introductions, meetings, presentations, and advocacy through WebVector's voice, paste, upload, or manual input methods. In Directed Mode, contributors CC or BCC the Catalyst agent on outgoing emails (e.g.,

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

qpncatalyst@inbound.webshield.io), triggering LLM extraction of structured fields and automatic creation of contribution records with the email as auto-attached evidence.

- **Engagement signal detection:** Three pre-milestone engagement signals — Meeting Requested, Introduction Requested, and Follow-up Sent — capture relationship-building activity that has not yet resulted in a confirmed milestone but demonstrates active progression. Engagement signals are recorded as contribution records with SENT status, eligible for upgrade to VERIFIED_ENGAGEMENT upon counterparty response, and further upgrade to confirmed milestone types (Introduction Made, Meeting Held, Partnership Agreement Signed) as the relationship advances. The SENT → VERIFIED_ENGAGEMENT → CONFIRMED_MILESTONE progression creates a granular timeline of relationship development that feeds cascade attribution.
- **AI Evaluation Pipeline classification:** Every outreach event — whether captured through Active Mode narration, Directed Mode email intake, or retrospective archaeology — is processed through the full three-stage pipeline: semantic classification against the contribution taxonomy using causal-enablement logic, identity enrichment for all referenced contacts and organizations, and temporal durability anchoring. The pipeline detects contribution type (introduction, advocacy, outreach, endorsement, referral, negotiation, follow-up), assesses cascade potential, and links the outreach to prior and subsequent contributions in the chain.
- **Retrospective communication archaeology:** Contributors export their full communication archive (email, messaging, calendar) to a secure local environment. The AI Evaluation Pipeline performs full-archive semantic analysis — not keyword filtering, but causal-enablement intent assessment — to identify communications that meet the contribution taxonomy criteria. For each qualifying interaction, a retroactive Trust Block is generated and signed by the local AI agent acting as a Proof-of-Analysis attestor. This enables recovery of attribution credit for historical outreach and advocacy that predates CommVector deployment — particularly valuable for contributors with years of relationship-building activity embedded in their email archives.
- **Privacy-preserving PII redaction:** All PII in CommVector records is redacted to opaque tokens before any transmission or sharing. Example: "Had a call with Sarah Chen at Google" → "Had a call with contact_hash_8f9a at org_hash_2c71." The zero-knowledge certificate format proves the contributor sent a message with qualifying characteristics (organizational level, outreach intent, domain) without revealing the content, recipient name, or employer.
- **Attachment processing:** PDF, Word, and image attachments accompanying outreach communications are processed by the AI Evaluation Pipeline alongside the message body. An MOU forwarded as a PDF attachment generates both a CommVector contribution record (for the outreach) and a DocVector-equivalent contribution record (for the signed agreement) from a single capture event. Evidence from attachments is hashed and linked to the contribution record, immediately qualifying for the Evidence Bonus.
- **Evangelized Mode distribution tracking:** Attribution-tracked distribution of awareness and participation content through any channel — EasyAccess Links embedded in email signatures, social media posts, blog articles, newsletter inclusions, conference presentations, partner communications, and influencer content. Each distribution event creates attribution-tracked enrollment and contribution pathways. When downstream participants engage and contribute, the contribution graph traces the cascade back to the evangelizer's distribution activity. The evangelizer earns Cascade Premium and Publicity Premium weighted Quantum Privacy Rewards proportional to the total settlement value their distribution generated.
- **Referral and Endorsement integration:** CommVector captures Referrals (the contributor connects a contact to a specific counterparty, Exchange Network, or opportunity without staking reputation) and Endorsements (the contributor attests to the quality, credibility, or capability of a contact, Resource, or proposal with reputation backing) as distinct contribution types with different attribution weights and accountability implications. Referrals create access-linkage edges in the contribution graph; Endorsements create reputation-staked edges that affect the endorser's behavioral Quantum Reputation based on outcomes.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Inbound email capture (Directed Mode):** The simplest path from a sent email to a contribution record requires no plugin, no browser extension, and no app installation. The contributor CCs or BCCs a QPN Catalyst capture address on any outgoing message. The system receives the email, processes it through the AI Evaluation Pipeline, and generates a draft attribution record for the contributor to confirm via the QPN Catalyst app or a reply link. Capture address formats include personal capture addresses (e.g., jh-a8f3@log.catalyst.qpn) routing exclusively to the contributor's QPC, and program-scoped addresses (e.g., lokahi@log.catalyst.qpn) attributing inbound messages to the program's contribution graph without exposing individual contributor identity.

QPN/PNX Implementation Role

CommVector is the primary capture module for relationship-intensive ecosystem formation — the introductions, advocacy, outreach, follow-ups, presentations, and negotiations that constitute the majority of early-stage QPN ecosystem-building activity. Where CodeVector captures what contributors build, DocVector captures what they formalize, and MeetVector captures what they discuss, CommVector captures what they initiate — the outbound activity that sets cascade chains in motion.

CommVector is particularly critical for the contribution categories that carry the highest Launch Premium weights: Executive Access & Introduction, External Advocacy & Amplification, and Ecosystem Orchestration. These categories are relationship-driven, communication-intensive, and historically untrackable — precisely because their value lies in the human relationship dynamics that occur between sending a message and receiving a commitment. CommVector's verified engagement loop transforms this invisible relationship work into a verifiable, settlement-eligible attribution chain.

The Evangelized Mode distribution tracking capability makes CommVector the operational engine for the Grassroots Evangelism-Ownership-Demand Cascade (Section 6.8). Every EasyAccess Link shared, every social media post advocating for QPN participation, every newsletter inclusion explaining the opportunity creates an attribution-tracked pathway that generates Quantum Privacy Rewards proportional to the downstream settlement it enables. CommVector provides the infrastructure through which the grassroots cascade scales from individual advocacy to population-level demand generation.

CommVector also forms the outbound half of a complete inbound-outbound attribution loop when paired with MessageVector (B.12.9). CommVector captures what the contributor sends; MessageVector captures what the counterparty sends back. Together they ensure that no communication-based contribution event is missed, whether the contributor initiates it or the counterparty does.

Incremental QPN Value Add

- **Attribution completeness for relationship-intensive contributors** — executives, business development professionals, consultants, investors, government relations leads, and ecosystem orchestrators whose most valuable work is outreach and advocacy receive verifiable, settlement-eligible attribution for activity that has historically been untrackable.
- **Verified engagement as confidence amplifier** — the SENT → VERIFIED_ENGAGEMENT status upgrade provides cryptographic proof that outreach produced a response, materially strengthening attribution confidence and cascade chain integrity. Contributors whose outreach generates verified engagement earn higher Quantum Privacy Rewards than contributors whose outreach remains unverified.
- **Grassroots cascade infrastructure** — Evangelized Mode distribution tracking through CommVector provides the operational foundation for the bottom-up adoption pathway, enabling individuals to earn Quantum Privacy Rewards proportional to the downstream settlement their advocacy generates.
- **Retrospective value recovery** — contributors with years of relationship-building activity embedded in email archives can retroactively capture attribution credit for historical outreach and advocacy, recovering value from ecosystem-building work that predates CommVector deployment.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Cross-module cascade initiation** — CommVector records serve as the originating node for cascade chains that subsequently pass through MeetVector (meetings), DocVector (signed agreements), CodeVector (implementations), and AgentVector (research and analysis), creating multi-module attribution chains with the highest cascade premium weights.
- **Referral and Endorsement attribution** — CommVector's distinct capture of Referrals and Endorsements feeds directly into the Quantum Reputation system, enabling contributors to grow their Catalyst Networks through both access-facilitation (Referrals) and quality-attestation (Endorsements) with appropriate accountability for each.
- **Zero-friction Directed Mode** — the CC/BCC email capture pathway requires no software installation, no browser extension, and no workflow change beyond adding an address to outgoing emails, making it the lowest-friction attribution mechanism in the entire Catalyst architecture.

Target Users

All contributors whose ecosystem-building activity involves outreach, introductions, advocacy, or relationship management: executives, business development professionals, strategy consultants, venture capital and private equity partners, government relations leads, policy advisors, ecosystem orchestrators, influencers, content creators, and any professional whose primary contribution is connecting people, organizations, and opportunities. Also: grassroots evangelists distributing awareness and participation content through personal and professional networks via Evangelized Mode.

Platforms

Email: Gmail, Outlook, Apple Mail, and any SMTP-accessible email client (via Directed Mode CC/BCC capture). Messaging: Slack, LinkedIn, WhatsApp, Signal, Telegram, iMessage, SMS. Professional networking: LinkedIn InMail, Twitter/X DMs. Social media and content distribution: any platform supporting EasyAccess Links for Evangelized Mode tracking. Active Mode capture: WebVector (voice, paste, upload, manual input methods) through QPN Catalyst.

Installed Base

Email is used by over 4.5 billion people globally — the single largest professional communication platform. Slack has over 30 million daily active users across enterprise and team environments. LinkedIn has over 1 billion members. WhatsApp has over 2.5 billion users. The combined communication platform installed base encompasses virtually every professional on earth. CommVector's Directed Mode CC/BCC capture requires no platform integration — it works with any email client on any device — making the addressable contributor base identical to the global email user population.

Total Addressable Value Enabled

Relationship-driven economic activity — introductions, advocacy, negotiations, and partnership formation — represents the initiation point for trillions of dollars in annual commercial value across every sector. The specific contribution categories CommVector captures (Executive Access, Ecosystem Orchestration, External Advocacy) generate the longest cascade chains and the highest cumulative settlement value in the Quantum Privacy Rewards framework, because a single introduction can trigger a cascade of meetings, agreements, implementations, and deployments that generate settlement value for years. Even attributing 1% of professional outreach and advocacy activity to PNX-connected Exchange Networks would represent hundreds of billions of dollars in traceable, settlement-eligible chain-initiation value — with the downstream settlement value of the cascades those chains produce being orders of magnitude larger. Evangelized Mode distribution tracking extends the addressable value to the entire consumer internet: every social media post, newsletter, blog article, and influencer endorsement that drives PPN enrollment and Exchange Network participation generates settlement-linked attribution.

Development Effort & AI Leverage

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Phase	Scope	Effort	AI-Automatable
Alpha / Phase 0	Active Mode capture through WebVector (voice, paste, manual narration of outreach events). Directed Mode email intake via CC/BCC capture address. AI Evaluation Pipeline classification of outreach and advocacy contributions. PII redaction to opaque tokens. Auto-evidence attachment for email and PDF attachments. Engagement signal detection (Meeting Requested, Introduction Requested, Follow-up Sent).	**1–2 dev-mo**	**~75%**
Beta / Phase 1	Verified engagement loop (SENT → VERIFIED_ENGAGEMENT) via Gmail and Outlook API polling for In-Reply-To matching. Evangelized Mode distribution tracking with EasyAccess Link attribution. Referral and Endorsement capture as distinct contribution types. Retrospective communication archaeology for email archive processing. Slack and LinkedIn messaging integration. Cross-module chain linkage to MeetVector and DocVector records.	**3–5 dev-mo**	**~65%**
GA / Phase 2	Full messaging platform coverage (WhatsApp, Signal, Telegram, iMessage, SMS) via platform APIs and virtual proxy numbers. Real-time verified engagement across all channels. Advanced cascade chain reconstruction linking outreach to downstream institutional outcomes. Enterprise Mode API deployment for server-side outreach classification. Institutional Mode bulk processing for enterprise communication archives.	**4–7 dev-mo**	**~60%**

The core AI classification and PII redaction logic reuses the existing AI Evaluation Pipeline with outreach-specific extraction prompts. Email intake via CC/BCC is architecturally simple and already operational in QPN Catalyst's Directed Mode. The primary human-intensive work involves verified engagement loop implementation (each email and messaging platform exposes reply-thread data differently), Evangelized Mode attribution chain construction (tracking downstream enrollment and contribution across arbitrary distribution pathways), retrospective archaeology pipeline optimization for large email archives, and messaging platform API normalization across providers with varying levels of thread and engagement data exposure.

B.12.8 MeetVector (Virtual Meeting & Transcript Attribution Engine)

Description

A privacy-preserving attribution engine that captures, classifies, and attributes contributions embedded in virtual meeting transcripts and AI-generated meeting summaries — transforming the richest, most strategically consequential class of professional activity into verifiable, QPC-signed contribution records. MeetVector bridges virtual meeting platforms (Zoom, Microsoft Teams, Google Meet, Webex, GoTo Meeting, Slack Huddles) and standalone AI meeting intelligence tools (Read.ai, Fireflies.ai, Otter.ai, MeetJamie.ai, Avoma, Fathom, Grain) with the QPN Accelerator Catalyst attribution infrastructure. It operates through two pathways: a general-purpose AI analysis pathway (immediate, no integration required) and a native platform integration pathway (end-to-end cryptographic provenance). Neither pathway transmits raw transcript content outside the contributor's security perimeter.

Capabilities

- **Transcript hashing and timestamping:** SHA-256 hash of the full transcript content signed with the contributor's QPC key at the moment of capture, establishing tamper-evident provenance before any human curation occurs. In Pathway 2 (native integration), the hash

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

is computed server-side at transcript generation time, providing cryptographically unbroken provenance from the meeting event to the attribution record.

- **AI-assisted contribution classification:** The Three-Stage AI Evaluation Pipeline runs against the full transcript or AI-generated summary, classifying meeting events against the Catalyst Contribution Taxonomy using causal-enablement logic. Speaker diarization from the meeting platform or AI meeting tool identifies which participant made which statements, enabling per-speaker contribution attribution. Confidence scores and cascade indicators are generated for each identified contribution event.
- **Commitment tracking and cross-module linkage:** AI-extracted action items and verbal commitments are recorded as COMMITMENT_STATED contribution records. Downstream execution evidence from other modules (DocVector-captured agreements, CodeVector-captured commits, CommVector-verified follow-up messages) automatically upgrades these records to COMMITMENT_VERIFIED, creating a cross-module cascade chain from verbal commitment to executed action.
- **Multi-participant identity enrichment:** All identified meeting participants are processed through the AI Evaluation Pipeline's Stage 2 Identity Enrichment pipeline. Known contacts are resolved against the contributor's CCP automatically; new participants trigger identity enrichment prompts. Organizational roles, reporting relationships, and affiliation attributes are captured for all participants with the contributor's explicit authorization, enriching the global contribution graph with the organizational reach of each meeting.
- **Retrospective archaeology for meeting archives:** Bulk retrospective processing of historical meeting transcripts stored in the contributor's Zoom, Teams, or AI meeting tool archive. The same causal-enablement classification pipeline applied to new meetings is run against the full historical archive, capturing contribution records for meetings that occurred before MeetVector was deployed. This is particularly valuable for contributors with months or years of recorded meetings containing unattributed executive introductions, advocacy activities, and technical validation work.
- **Cross-verification integration:** Meeting participants identified as counterparties in attributable contributions receive standard Cross-Verification Protocol requests (B.7) through their preferred channels. Confirmed participants are added to the contribution graph as independent nodes with their own cascade-eligible attribution records. The meeting transcript hash serves as the shared evidence artifact — both parties can reference the same cryptographically signed transcript to corroborate their respective contributions.

QPN/PNX Implementation Role

MeetVector closes the most significant attribution gap in the current contribution capture architecture: the invisibility of verbal, in-meeting contributions. Without MeetVector, a contributor who spends 90% of their QPN-enabling work in meetings — briefing executives, facilitating multi-party alignments, driving technical validation discussions, negotiating commercial terms — generates almost no capture-layer evidence of that work. Every email they send is captured by CommVector; every document they sign is captured by DocVector; every line of code they commit is captured by CodeVector. But the conversation in which the executive decided to commit, the meeting in which the architect validated the approach, and the call in which the commercial terms were agreed: these were invisible. MeetVector makes them visible.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

MeetVector is particularly critical for the contribution categories most dependent on in-person and virtual interaction: Executive Access & Introduction, Internal Advocacy & Facilitation, Ecosystem Orchestration, and Commercial Term Negotiation. These categories generate the highest cascade premiums but produce the least written evidence — precisely because their value lies in human relationship-building that has historically been untrackable. MeetVector transforms relationship capital into attributable, verifiable, settlement-eligible contribution records.

Incremental QPN Value Add

- Attribution completeness for relationship-intensive contributors — executives, business development leads, ecosystem orchestrators, and governance specialists whose most valuable work occurs entirely in meetings can now generate a complete, verifiable contribution record without changing their workflow.
- Cross-module cascade amplification — verbal commitments captured by MeetVector that subsequently result in executed agreements (DocVector), code submissions (CodeVector), or verified follow-up communications (CommVector) create multi-module cascade chains with the highest achievable attribution confidence scores.
- Retrospective value recovery — contributors with years of recorded meeting archives can retroactively capture contribution records for work that predates MeetVector deployment, recovering attribution credit for historical ecosystem-building activity that would otherwise remain unrecorded.
- AI meeting tool competitive incentive — meeting platform vendors and AI meeting intelligence providers that integrate MeetVector natively earn Quantum Privacy Rewards (Reusable Infrastructure Development category) and give their enterprise customers higher attribution confidence scores, creating a market differentiator that accelerates adoption of native integration across the meeting platform ecosystem.
- DLP-compatible enterprise deployment — because raw transcript text never leaves the contributor's security perimeter, MeetVector is deployable within enterprise environments subject to Data Loss Prevention controls without triggering data classification or transmission restrictions.

Target Users

All contributors whose primary QPN-enabling activity occurs in virtual meetings: executives, business development professionals, strategy consultants, ecosystem orchestrators, compliance specialists, technical architects, government relations leads, and enterprise sales professionals. Also: enterprise program managers and project leads who run recurring multi-stakeholder coordination calls where QPN adoption decisions are being shaped in real time.

Platforms

- **Virtual meeting platforms:** Zoom, Microsoft Teams, Google Meet, Cisco Webex, GoTo Meeting, Slack Huddles.
- **AI meeting intelligence tools:** Read.ai, Fireflies.ai, Otter.ai, MeetJamie.ai, Avoma, Fathom, Grain, Chorus.ai, Gong.
- **General-purpose AI analysis:** Claude, ChatGPT, Gemini, Grok (via document upload with EP3 Contribution Context loaded).

Installed Base

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Zoom serves 300M+ daily meeting participants. Microsoft Teams has 320M+ monthly active users. Google Meet processes 3B+ minutes of video calls daily. The combined installed base of these three platforms alone spans virtually every Global 2000 enterprise. AI meeting intelligence tools are growing rapidly: Read.ai, Fireflies.ai, and Otter.ai collectively serve tens of millions of users; Gong and Chorus serve enterprise sales organizations with 70,000+ customers combined. The total addressable contributor base for MeetVector integration is larger than any other Capture Tool surface — because every professional who uses any of these platforms is a potential contributor, and no additional software or workflow change is required beyond enabling the integration.

Total Addressable Value Enabled

MeetVector does not directly enable a distinct category of resource settlement (unlike, for example, the Unity Catalog Bridge which enables data asset settlement). Instead, it dramatically increases the completeness and confidence of attribution records for the highest-value contribution categories: Executive Access & Introduction, Internal Advocacy & Facilitation, and Ecosystem Orchestration. Because these categories carry the highest Launch Premium weights and generate the longest cascade chains, even a 20% increase in attribution confidence across these categories translates to materially higher Quantum Privacy Rewards for contributors whose work is currently under-attributed — and materially better cascade chain reconstruction for the Global Graph Assembly Engine. The net effect is a more accurate, more complete, more densely connected global contribution graph, which increases the precision and fairness of all Quantum Privacy Rewards allocation across the entire ecosystem.

Development Effort & AI Leverage

Prototype	Controlled Beta	GA Release	AI-Automatable
1–2 months	**2–4 months**	**4–6 months**	**60–70%**

Development effort is estimated across three phases:

- **Prototype / Alpha (1–2 dev-months):** Pathway 1 (general-purpose AI analysis via document upload) and a single Pathway 2 integration (Zoom transcript webhook or Fireflies.ai API). Covers the core AI Evaluation Pipeline Classification Stage applied to transcript content, .qpn archive storage, and basic participant identity enrichment. AI-automatable share: ~70%.
- **Controlled Beta (2–4 dev-months):** Full platform coverage for the top-5 virtual meeting platforms and top-5 AI meeting tools. COMMITMENT_STATED/COMMITMENT_VERIFIED cross-module linkage. Cross-verification integration for multi-participant meetings. Retrospective archaeology for historical meeting archives. Enterprise Mode C (server-side API) deployment. AI-automatable share: ~65%.
- **GA Release (4–6 dev-months):** Full platform coverage including long-tail meeting tools. Meeting Bot participant integration for server-side transcript capture. Real-time in-meeting classification (live contribution identification during the meeting, not post-hoc). Enterprise graph densification through Private Accelerator meeting integration. AI-automatable share: ~60%.

The core classification and attribution logic reuses the existing Three-Stage Evaluation Pipeline with minimal modification — transcript content is simply a new input format for the same semantic classification engine. The primary engineering work is in building and maintaining platform API integrations (webhook handlers, OAuth flows, schema normalization across provider formats) and the cross-module COMMITMENT_STATED/COMMITMENT_VERIFIED

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

linkage logic. Both are well-suited to AI-assisted development and follow well-documented vendor API specifications.

B.12.9 MessageVector (Universal Messaging Proxy & Attribution Capture Network)

Description

A privacy-preserving proxy network that enables any communication channel — email, messaging, fax, or physical mail — to route inbound messages to the QPN Catalyst attribution pipeline without the sender ever interacting with a QPN system or being aware that attribution is occurring. MessageVector provisions an arbitrary number of proxy addresses (email, messaging, fax, and physical) in personal, enterprise, or third-party domains, with per-contributor and per-contact routing tokens that attribute inbound messages to the correct QPN participant automatically. Server-side Privacy Pipe relay ensures the forwarding is undetectable at the network level. All inbound content is processed through the AI Evaluation Pipeline for OCR, semantic classification, entity resolution, and Attribution Record generation, with compliance screening by PPCS and FCFPS before records are activated.

The Catalyst Proxy Network is formally authorized as a governed capability of the QPN Catalyst Network. Proxy addresses are designed to be shared freely — that is the point of the proxy network: to facilitate evangelism, provide familiar submission paths from the participant's own domain, and attribute the resulting contribution graphs to the participant who established the proxy. Registration of an Authorized Catalyst Proxy Address constitutes a Contribution Record attributable to the registering participant, and all communications routed through the proxy are linked to that participant's contribution graph for chain origination attribution. The Catalyst Submission Terms apply to all communications sent to proxy addresses. Proxy operators have the option — but not the obligation — to keep their proxy's connection to the Catalyst Network private. Participants building a contribution graph within an organization who want to protect their team's competitive strategy can rely on the confidentiality and trade-secret protections to keep the forwarding destination and Catalyst connection private. Alternatively, participants can be fully transparent about the proxy's purpose. The choice is the proxy operator's. Regardless of the proxy operator's disclosure choices, the identity of individuals who have submitted through the proxy is always protected — their submission activity is their competitive information.

Target Users

All contributors, with particular value for: enterprise contributors behind DLP controls who cannot install client-side tools; relationship-intensive contributors (executives, government relations leads, business development) whose counterparties send high-value documents (MOUs, LOIs, signed agreements) by email, fax, or physical mail; contributors who want passive attribution capture without ongoing manual effort; and any contributor introducing contacts who should never be directly aware of QPN Catalyst.

Development Effort & AI Leverage

Phase	Scope	Effort	AI-Automatable
Alpha / Phase 0	Email ingest (SMTP), personal proxy address provisioning, D.4 CC/BCC capture, AI Evaluation Pipeline processing of plain text and PDF attachments, VoiceVector app confirmation flow.	**1–2 dev-mo**	**~70%**
Beta / Phase 1	Referral Proxy provisioning and routing token system. Custom domain forwarding and Privacy Pipe relay. Messaging platform proxies (virtual phone numbers for SMS/WhatsApp). eFax virtual number provisioning and PDF-to-attribution pipeline. Compliance screening integration (PPCS/FCFPS) for inbound records.	**2–4 dev-mo**	**~60%**

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

GA / Phase 2	Physical mail processing service integration. Signal/iMessage proxy support. Full OCR pipeline for handwritten and complex document formats. Multi-contributor shared program address management. Anomaly detection tuning for proxy-specific fraud patterns.	**4–6 dev-mo**	**~55%**

B.12.10 Catalyst Assistant (AI-Assisted Contribution Drafting & Evangelism Engine)

Description.

An AI-powered drafting system that provides installable Skills for Claude, OpenAI, and OpenClaw, helping contributors draft communications that are simultaneously optimized for human readability and for the Catalyst extraction pipeline. The assistant operates on the email channel during Phase 0 with zero backend dependency, addressing the two primary sources of Contribution Ledger incompleteness: contributions that are never recorded (because the contributor forgot or didn't realize the interaction qualified) and contributions that are recorded but too vague for reliable AI extraction (first names without organizations, missing context, unclear purpose).

Capabilities.

Dual-purpose drafting: every email reads as a natural business communication while including structured data the pipeline expects. Two-layer evangelism: platform-level launch evangelism and accelerator-level program evangelism. Accelerator-aware operational skills: four contribution patterns (introduction/referral, meeting follow-up, partnership/MOU, general capture) in accelerator-specific variants. Shared knowledge base: contribution taxonomy, extraction field definitions, email structure best practices, and program context maintained once and consumed by all skills.

Delivery Phases.

- Phase 1 (under active development): Individual AI Skills for Claude, OpenAI, and OpenClaw. Tested across six scenarios. No backend required.
- Phase 2: Unified plugin with routing, session memory, batch recording, portfolio queries, slash commands. Depends on Catalyst API Service.
- Phase 3: Browser extension, Custom GPTs, MCP integration, additional accelerator-specific skills.

QPN/PNX Implementation Role.

Primary vehicle for multi-surface distribution and lowest-friction attribution mechanism for relationship-intensive contributors. Operational infrastructure for the Grassroots Cascade: evangelism skills equip every contributor to explain the ownership model and recruit new participants.

Phase	Scope	Effort	AI-Automatable
Phase 1 (Active)	Individual skills for Claude, OpenAI, OpenClaw. General and Lokahi-specific operational skills. Launch evangelism skill. Shared knowledge base. Test framework.	**1–2 dev-mo**	**~75%**
Phase 2	Unified plugin with routing, session memory, batch recording, portfolio queries, slash commands. Depends on Catalyst API Service.	**2–3 dev-mo**	**~65%**
Phase 3	Browser extension, Custom GPTs, MCP integration, additional accelerator-specific skills.	**3–5 dev-mo**	**~60%**

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

APPENDIX C - *Value Accrual Framework, Universal Ownership & Participation Strategy*

C.0 Purpose & Analytical Framework

This appendix provides a structured analytical framework for assessing and quantifying the total ecosystem value, direct economic capture, Quantum Privacy Rewards potential, and cost of delay for any prospective QPN/Accelerator participant — whether an enterprise, technology vendor, professional services firm, financial institution, sovereign entity, or individual contributor.

The framework is designed to be applied systematically by analysts, strategists, or AI-assisted evaluation tools to generate participant-specific launch strategies and economic projections. For any given potential participant, the analysis proceeds through five steps:

- **Step 1 — Ecosystem Magnitude Assessment.** Using the Three-Channel Value Framework (Section C.1), estimate the total PNX-settled value that would flow through the participant's ecosystem as a Tier 1 Accelerator anchor. This requires evaluating: (a) cross-vertical reach — how many sectors does the participant's ecosystem touch, (b) settlement density — what fraction of PNX-settled activity would route through infrastructure, models, or services this participant provides, and (c) topology positioning — how early and how durable is the participant's position under preferential attachment dynamics.
- **Step 2 — Direct Capture vs. Ecosystem Distribution.** Using the Allocation Waterfall and Strategic Commitment Spectrum (Section C.2), decompose the total ecosystem magnitude into: direct Anchor capture (the share flowing to the participant's shareholders through Accelerator Tokens and Participant Pool dominance), ecosystem participant capture (the share flowing through Universal Ownership to employees, customers, vendors, and partners), and public benefit flows (the share flowing to the EP3 Nature & Humanity Trust).
- **Step 3 — Quantum Privacy Rewards Projection.** Using the Launch Premium, Governance Premium, and Adaptive Premium definitions from Section 4 of the main document, project the Quantum Privacy Rewards attributable to the specific individuals and contribution graphs that enabled the participant's activation — including the Strategic Premium for securing the Anchor commitment, the Timing Premium reflecting when the commitment occurs relative to competitors, the Cascade Premium for downstream adoption the commitment triggers, and the Proportionality Premium adjustment as the participant's category becomes less scarce.
- **Step 4 — Laggard Penalty Quantification.** Using the Tier 1 vs. Laggard differential (Section C.1) and Competitive Exclusion Dynamics (Section 3.6 of the main document), calculate the economic penalty for delay: the 70–85% discount that applies when a participant enters after Tier 1 positioning is captured by competitors, the compounding erosion of trust taxonomy anchoring, and the permanent forfeiture of routing centrality that early entrants accumulate.
- **Step 5 — Launch Strategy Generation.** Using the Race Dynamics (Section 3), the Embryonic Network Incubation pattern (Section A.13), and the participant's specific ecosystem topology, generate a concrete adoption strategy: which relationships to activate first, which contribution graphs to pursue, which Accelerators to join or form, and what the optimal balance between bottom-up incubation and top-down executive sponsorship looks like for this participant's organizational context.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

This framework can be applied by human analysts or used as structured context for AI-assisted strategy generation. When provided to an LLM along with the participant's specific characteristics (industry, market position, existing relationships, data assets, technology stack, regulatory environment), it enables the generation of detailed, participant-specific launch plans with quantified economic projections for early adoption versus delay.

C.1 Ecosystem Valuation Metrics Framework

The projected economic value for each Anchor participant is derived from a structured set of valuation metrics, each grounded in a distinct operational mechanism within the QPN architecture and traceable to specific positions in the PNX Settlement Waterfall (Section 4.8). Together, these metrics define the total ecosystem magnitude, the structural drivers of first-mover advantage, the specific QP Token rights that generate value, and the mechanisms by which early participation translates into durable ownership.

The framework is organized into two tiers: **Summary Valuation Metrics** that aggregate the opportunity into decision-grade quantities, and **Input Value Metrics** that decompose those aggregates into their constituent operational mechanisms — each traceable to a specific QP Token type, Exchange Token flow, or conventional revenue stream.

Summary Valuation Metrics

These are the high-level metrics used in Ecosystem Assessments, slide decks, and investment memoranda to summarize the opportunity for Accelerator Network Participants.

- **Anchor Ecosystem Value** — The aggregate NPV of all QP Token rights and economic flows derived from activating the Anchor's products, resources, user population, and its customer, partner, and vendor ecosystems through the Accelerator Network and PNX settlement.

  This is the total economic magnitude flowing through the Anchor's ecosystem topology within the PNX — the sum of all Input Value Metrics described below. It represents the value of the graph of QP Token rights rooted in the Anchor organization or person, realized through participation in Exchange Networks, Resource Pools, and ongoing PNX Settlement via Exchange Tokens. In formal contexts: "Tier 1 Anchor Ecosystem Value" for entities that commit during the launch window; "Laggard Ecosystem Value" for entities that delay.

  Anchor Ecosystem Value is not shareholder value. As detailed in Section C.2, economic rights are distributed across every participant who contributes to the activation, operation, and ongoing performance of Exchange Networks and Resource Pools within the Anchor's ecosystem. The allocation follows the verified contribution graph — not the organizational chart. How much of Anchor Ecosystem Value flows to the Anchor's direct stakeholders depends on the nature and aggressiveness of the Anchor's participation, as described in the Strategic Commitment Spectrum (Section C.2).

  The key scaling variables for Anchor Ecosystem Value are:

  (a) **cross-vertical reach** — how many sectors the entity's ecosystem touches, which determines the breadth of PNX-settled activity that flows through its topology;

  (b) **settlement density** — what fraction of PNX-settled activity would route through infrastructure, models, or services the entity provides, which determines the depth of value capture within each sector; and

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

(c) **topology positioning** — how early and how durable the entity's position is under the preferential attachment and accreditation sequencing dynamics that govern Exchange Network formation and routing preference.

An entity with broad cross-vertical reach, high settlement density, and early topology positioning will have a substantially larger Anchor Ecosystem Value than an entity that is narrow, substitutable, or late.

- **Catalyst Rewards Pool** — The aggregate NPV of the Accelerator Incentive & Investment Pool value available to Catalyst participants connected to the Anchor Commitment, both upstream in establishing the Anchor Commitment (introductions, advocacy, partnership development, executive engagement) and downstream in translating the commitment into resource activation, ecosystem onboarding, and ongoing PNX settlement. Each QPN Catalyst participant can participate in and receive QP Rewards allocations from any of the shared Accelerator Pools, and can also create their own Private Accelerators, each of which has a minimum 5% Incentive Pool available for allocation through the QPN Catalyst Network, with the remaining rights to the Private Accelerator allocated based on the model or process defined by its managers. In formal contexts: “Tier 1 Catalyst Rewards Pool.”

  The Catalyst Rewards Pool is a subset of Anchor Ecosystem Value — specifically, it represents the portion of the 20% Accelerator Incentive & Investment Pool that is allocated through the QP Rewards framework rather than through direct financial investment. It is the primary metric for evaluating what individual contributors and innovation catalysts can earn by driving Anchor participation.

- **Anchor Direct Capture** — The portion of Anchor Ecosystem Value available for allocation to the Anchor’s direct stakeholders — shareholders, token holders, employees, investors, executives, board members, advisors, and consultants — through Accelerator Tokens, Participant Pool dominance, and operational Exchange Token flows. Direct capture typically represents 25–40% of Anchor Ecosystem Value for dominant infrastructure anchors, 20–35% for trust and governance anchors, and 10–20% for infrastructure substrates (where the value proposition depends on the breadth and diversity of participants building on the platform). The remaining 60–80%+ flows to ecosystem participants through Universal Ownership — the employees, customers, vendors, partners, and individual contributors whose verified contributions enable, amplify, and sustain the Anchor’s ecosystem topology. In formal contexts: “Tier 1 Anchor Direct Capture.”

- **Anchor Value Multiple** — The ratio of Anchor Direct Capture to the entity’s current valuation. For publicly traded companies, current valuation is market capitalization. For private companies, it is estimated valuation based on revenue, margins, comparable private-market transactions, or recent funding rounds. For partnerships and professional services firms, it is estimated based on revenue multiples appropriate to the firm’s sector. For sovereigns, non-profits, membership organizations, and philanthropic entities, appropriate alternative denominators may include annual budget, assets under management, endowment value, or revenue — selected based on what best represents the entity’s current economic scale. The Anchor Value Multiple quantifies the magnitude of the opportunity relative to the entity’s existing value, making it the single most compelling metric in executive presentations: a Value Multiple of 10x means the entity’s participation in the QPN could generate ten times its current value in QP Token rights.

- **Laggard Penalty** — The percentage reduction in expected Anchor Ecosystem Value for an entity that delays participation past the Tier 1 anchor window. Laggard Penalties reflect

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

architectural properties of the PNX where early allocation is durable and non-replicable: Incentive Pool closure is time-bound, trust taxonomy lock-in compounds through preferential attachment, and routing preference accumulates at early nodes in ways late entrants cannot replicate. Typically 70–85% for enterprise anchors, meaning a laggard captures only 15–30% of what a Tier 1 anchor captures.

The Laggard Penalty applies differently to enterprises and individuals:

Enterprise Laggard Penalty — The percentage reduction of the expected Anchor Ecosystem Value for an enterprise that does not join until after the Enterprise Cascade of Accelerator Participation, instead of committing as a Tier 1 Anchor. This reflects the loss of Incentive Pool access (fully locked for early participants), the diminished topology positioning (preferential attachment has already concentrated routing at early nodes), and the reduced trust taxonomy influence (governance standards have already been authored by earlier participants).

Individual Laggard Penalty — The reduction in expected value of Catalyst Contributions from the Pioneer Rewards phase until after the Adoption Cascades trigger and the available pool of such contributions expands dramatically. During Pioneer Rewards (Premium Multiple 100–1,000x+), contributions sit at the root of cascade graphs that propagate into enormous downstream settlement value. After cascades trigger, the Premium Multiple drops to 10–50x and continues declining — not because later contributions are unimportant, but because the scarcity compression and declining marginal cascade value of early contributions are no longer available.

Input Value Metrics

These are the operational-level metrics that decompose Anchor Ecosystem Value into its constituent value-generation mechanisms. Each Input Value Metric maps to a specific position in the PNX Settlement Waterfall (Section 4.8), a specific QP Token type, or a specific conventional revenue stream — making the connection between the summary metrics and the underlying value drivers explicit and traceable.

Estimation Direction: Bottom-Up Aggregation. When applying this framework to a specific entity, the Input Value Metrics should be estimated independently and aggregated upward to produce the Summary Valuation Metrics — not the reverse. Each Input Value Metric is governed by entity-specific scaling variables (pricing gap magnitude, convertible activity volume, trust anchor credibility, cross-vertical reach, ecosystem resource complementarity) that differ materially across entities and cannot be reliably inferred by decomposing an aggregate estimate. An entity's Anchor Ecosystem Value is the sum of its eight Input Value Metrics, each estimated from the entity's specific product offerings, infrastructure position, ecosystem composition, governance credibility, and commitment strategy. The Summary Valuation Metrics (Anchor Direct Capture, Value Multiple, Catalyst Rewards Pool, Laggard Penalty) are then derived from Anchor Ecosystem Value using the Allocation Waterfall and commitment-level-dependent capture ratios described in Section C.2. As a validation step, the aggregated Anchor Ecosystem Value should be cross-checked against the top-level scaling heuristic — cross-vertical reach × settlement density × topology positioning — to verify that the bottom-up sum falls within a plausible range. Where the bottom-up aggregate differs materially from the top-down estimate, the analyst should identify which Input Value Metrics are driving the divergence and assess whether the entity-specific assumptions are justified or whether the top-level scaling variables need recalibration.

The Input Value Metrics also describe the mechanisms by which early QPN Catalyst participation translates into a durable ownership stake — locking in ongoing flows of value

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

relative to later participants. Some metrics produce "locked" value (permanent QP Token positions), others produce "flowing" value (persistent but gradually diluting operational streams), and others produce conventional business value outside the PNX settlement system.

- **Incentive Pool Value** — Value derived from Accelerator Tokens allocated as QP Rewards via the QPN Catalyst Network from Accelerator Incentive & Investment Pools. This is the most direct connection between Catalyst participation and QP Token ownership: contributions that establish Anchor Commitments, drive resource activation, and advance the Accelerator's objectives are rewarded with Accelerator Tokens representing a permanent share of the Exchange Token flows generated by the Exchange Networks and Resource Pools incubated by the Accelerator.

  Incentive Pool Value contributes to Anchor Ecosystem Value, feeds the Catalyst Rewards Pool, and — to the extent allocated to direct Anchor stakeholders — contributes to Anchor Direct Capture. The waterfall position is the 20% Accelerator Incentive & Investment Pool described in Section 4.8.

  ***Lock mechanism**:* Incentive Pool Value locks when Accelerator Pools are allocated and fully locked, yielding rights to a fixed percentage of the Exchange Token stream from the Accelerator's Exchange Networks and Resource Pools. Once locked, these positions are permanent and non-dilutable within the Accelerator — they represent perpetual fractional ownership of the Accelerator's settlement flows, not a one-time allocation. This is the primary mechanism by which early Catalyst participation converts into durable ownership.

- **Investment Value** — Value derived from financial investment in Accelerators (whether shared or private), including direct equity or token investment in specific Accelerators, conversions or exchanges of Accelerator Token rights through Liquidity Pools, and early-stage financing through the Quantum Privacy Investment Network, which holds a right of first refusal on any investments into shared Accelerators.

  Investment Value contributes to Anchor Ecosystem Value, and the portion sourced from direct Anchor stakeholders contributes to Anchor Direct Capture. Like Incentive Pool Value, it maps to the 20% Accelerator Incentive & Investment Pool in the settlement waterfall, but represents the financial-investment share of that pool rather than the QP Rewards share.

  ***Lock mechanism**:* Investment Value locks alongside Incentive Pool Value when Accelerator Pools are allocated. Financial investors receive Accelerator Tokens representing their proportional share of the Pool, which yield perpetual rights to the Exchange Token stream from the Accelerator's settlement activity.

- **Exchange Network Value** — The incremental value stream derived from ongoing participation in Exchange Networks, producing a premium stream of Exchange Tokens from PNX Settlement. This captures the compounding operational advantages of early Exchange Network formation: routing centrality (early Exchange Networks attract more settlement traffic), preferential attachment (new participants preferentially connect to established Exchange Networks), and Monetization Uplift Multiple amplification (early Exchange Networks accumulate Proof-of-Trust history and reuse relationships that make their settlement flows progressively more valuable per unit of activity).

  Exchange Network Value maps to the 80% Participant Pool share of Accelerator-governed settlement and to the 100% participant share of organic (non-Accelerator) settlement, as described in Section 4.8. It flows through Exchange Tokens earned by Exchange Providers

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

(30% of post-Root settlement) and Resource Providers (70% of post-Root settlement) within each Exchange Network.

Persistence: Exchange Network Value is persistent because early positioning creates compounding routing advantages, but it is generally declining in relative share as the Exchange Network population grows and dilutes individual positions. Absolute value may continue increasing as total PNX settlement volume grows faster than the relative share declines. Early Exchange Network participants carry their accumulated Proof-of-Trust history, reuse relationships, and routing preference into the Open Exchange — competing at greater scale and higher margins than new entrants building from scratch.

- **Resource Pool Value** — The incremental value stream derived from the ongoing reuse of QP Resources and Resource Derivatives in Resource Pools — whether directly contributed by the Anchor's ecosystem or generated through the operation of Exchange Networks the Anchor participates in.

  Early Resource contributions and their Derivatives tend to be default components of Accelerator-incubated Exchange Networks, making them utilized by default in any settlement activity that those networks enable. Furthermore, the utilization of Resources often generates new Resource Derivatives incorporating data, insights, and computational outputs that are byproducts of user interaction or process automation through Personal or Enterprise Privacy Networks — resources that are not available from external enterprise sources and that create a compounding pool of proprietary reusable assets. Each derivative inherits the Trust Block lineage of its upstream Resources, ensuring that the governance architecture authored by early participants propagates into an expanding tree of settlement-generating assets.

  Resource Pool Value maps to the Resource Provider share (70% of post-Root settlement) of Exchange Token allocations. It is persistent but generally declining in relative share as the Resource Pool population expands, with the compounding effects of derivative generation partially offsetting the dilution.

- **Reputation Premium Value** — The incremental value attributable to the strengthening and expansion of Quantum Reputations through early Accelerator participation. Stronger Quantum Reputations increase the stream of Exchange Tokens from PNX operations through three mechanisms: preferential attachment (participants with higher reputations attract more counterparties and settlement volume), routing centrality (higher-reputation Exchange Networks and Resource Pools are preferentially selected for settlement routing), and UTM Premium amplification (the Unified Trust Model Premiums — Strategic, Timing, Value, Cascade, Governance, and Publicity — compound more strongly for participants with verified, high-reputation contribution histories).

  Reputation Premium Value does not map to a separate waterfall position — it amplifies the Exchange Token flows earned through Exchange Network Value and Resource Pool Value. It is persistent but gradually normalizing as the reputation distribution matures and the differential advantage of early reputation diminishes relative to the growing population of credible participants.

- **Settlement Model Value** — The incremental value derived from converting existing pricing models to outcome-level, settlement-linked economics through the PNX. When an entity's products, infrastructure, or services are consumed through PNX-settled Exchange Networks rather than through conventional pricing (subscriptions, licensing, metered transactions, capacity reservations), the value captured per unit of activity increases — often by orders of magnitude — because PNX settlement prices the *outcome* produced by

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

the combined resources of the Exchange Network, not the *input cost* of any single participant's contribution.

For Hedera, as an example, this means shifting from micro-payment metered consensus transactions to outcome-level value-sharing based on the combined resources of its ecosystem partners — capturing a share of the economic value of every settlement event routed through Hedera infrastructure, rather than a fraction-of-a-cent transaction fee. For a cloud provider, it means converting reserved compute capacity into settlement-linked Resource Pool economics where revenue reflects the value of the insights, predictions, and decisions the compute enables, not the hourly cost of the hardware. For an AI vendor, it means converting per-token API pricing to settlement-linked economics where revenue reflects the productivity gains and new value the AI creates for enterprises and individuals.

Settlement Model Value is PNX-settled and produces Exchange Tokens. It maps to the Resource Provider share (70% of post-Root settlement) and Exchange Provider share (30% of post-Root settlement) within Exchange Networks where the entity's resources are consumed. It is driven by four structural mechanisms: zero-marginal-cost access and reuse of dual-use enabling resources from ecosystem partners, superior value capture through end-to-end personalization and optimization across organizational boundaries, low-friction distribution through Exchange Networks and EasyAccess, and a more lucrative value-sharing model than existing pricing constructs permit.

***Persistence**:* Settlement Model Value is persistent and potentially compounding, because the conversion to settlement-linked economics is structural — once an entity's resources are published as QP Resources and consumed through Exchange Networks, the superior economics create switching costs that make reversion to conventional pricing irrational. However, the entity's *share* of total PNX-settled value from this mechanism may decline as more entities convert their own business models, diluting any single entity's relative position.

- **Dual-Use Revenue Value** — The incremental revenue derived from participants' dual-use operations that are not settled through the PNX but represent economic value enabled by QPN capabilities. This includes increased demand for existing products and services driven by the entity's QPN positioning (e.g., increased demand for Hedera consensus and token services as the default PNX settlement platform), new customer acquisition driven by Proof-of-Trust accreditation and privacy guarantees, efficiency gains from automated compliance and governance, competitive moat strengthening from deep integration with PNX-settled Exchange Networks, and customer retention driven by superior privacy and trust infrastructure.

  Dual-Use Revenue Value contributes to Anchor Ecosystem Value and, when earned by Anchor stakeholders, to Anchor Direct Capture. It is not token-backed — this is conventional business value flowing through existing revenue channels, not QP Token rights or Exchange Token allocations.

  ***Persistence**:* Dual-Use Revenue Value is persistent and grows with the entity's QPN ecosystem position, but it accrues through conventional business dynamics (market share, pricing power, customer loyalty) rather than through QP Token mechanics.

- **Ecosystem Growth Value** — The incremental value driven by increased user enrollment and enterprise ecosystem growth enabled by early QPN adoption through Accelerators. Larger user populations generate more PNX settlement activity, more Resource contributions, and more Exchange Network formation — all of which amplify every other Input Value Metric. This captures the demand-side effects of ecosystem expansion: each

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

new user, enterprise, or partner that joins the Anchor's ecosystem increases the total settlement volume flowing through the Anchor's topology, compounding the value of every locked and flowing position the Anchor and its stakeholders hold.

Ecosystem Growth Value is persistent and compounding during growth phases, stabilizing at ecosystem maturity. It contributes to Anchor Ecosystem Value by increasing the total magnitude that all other Input Value Metrics operate on — it is a multiplier, not an additive component.

Value Durability Classification

The Input Value Metrics fall into three categories based on how their value persists over time:

- **Locked Value** — Durable ownership via QP Token rights that yield perpetual claims on Exchange Token flows. Incentive Pool Value and Investment Value lock when Accelerator Pools are allocated and fully locked. Once locked, these positions represent a fixed percentage of the Exchange Token stream from the Accelerator's Exchange Networks and Resource Pools — permanent, non-dilutable within the Accelerator, and growing in absolute terms as settlement volume increases. Locked Value is the most direct mechanism by which early participation converts into durable ownership.
- **Flowing Value** — Persistent operational value streams that are durable but gradually declining in relative share. Exchange Network Value, Resource Pool Value, Settlement Model Value, and Reputation Premium Value represent ongoing Exchange Token flows earned through operational participation. They are persistent because early positioning creates compounding advantages (routing centrality, Proof-of-Trust history, reuse relationships, structural switching costs from settlement-linked economics), but they decline in relative share as the ecosystem grows and new participants enter. Absolute value may continue increasing as total PNX settlement volume grows. Early participants carry structural advantages into the Open Exchange that late entrants cannot replicate, but these advantages diminish asymptotically rather than holding constant.
- **Conventional Value** — Economic value flowing through existing business channels, not QP Token rights. Dual-Use Revenue Value and the business-uplift component of Ecosystem Growth Value accrue through conventional revenue, margin expansion, and competitive positioning. They are economically real and may be substantial — particularly for entities whose QPN positioning drives increased demand for existing products and services — but they are not settled through the PNX waterfall and do not produce Exchange Token allocations.

Aggregation and Tier 1 vs. Laggard Differential

Anchor Ecosystem Value is the sum of all eight Input Value Metrics and represents the total NPV flowing through the Anchor's ecosystem as a Tier 1 Accelerator anchor, on the specified valuation horizon (30-year NPV through 2056 as default, with 74-year NPV through 2100 as optional extended horizon, and annual value flows available for time-series visualization).

The Input Value Metrics are additive by construction — each maps to a distinct operational mechanism and a distinct position in the settlement waterfall or conventional revenue stream. There is no double-counting: Incentive Pool Value and Investment Value flow through the 20% Accelerator Pool; Exchange Network Value and Resource Pool Value flow through the 80% Participant Pool and 100% organic settlement; Reputation Premium Value amplifies (but does not duplicate) the Exchange Token flows captured by Exchange Network and Resource Pool Value; Dual-Use Revenue Value captures conventional revenue outside the PNX; and Ecosystem Growth Value captures the demand-side multiplier effect on all other metrics.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

The Laggard Penalty is derived by comparing the Tier 1 Anchor Ecosystem Value against the Laggard Anchor Ecosystem Value — the same metrics computed under the assumption that the entity delays past the Tier 1 launch window. The penalty reflects three architectural properties of the PNX that make early allocation durable and non-replicable:

- **First, Incentive Pool economics are front-loaded and time-sensitive**. As Tier 1 Anchor Commitments are secured and Adoption Cascades trigger, the Premium Multiple — the ratio of QP Rewards earned per unit of contribution effort compared to steady-state — declines steeply from 100–1,000x+ during Pioneer Rewards to 10–50x during Cascade Propagation and 2–5x during Automated Settlement. Simultaneously, the valuation of Accelerator Incentive Pools increases dramatically as each Anchor Commitment expands the settlement magnitude flowing through the Accelerator's Exchange Networks and Resource Pools. The combined effect is that a laggard making a contribution comparable to one made by an early participant receives a fraction of the QP Rewards — not because the pool is exhausted, but because the same pool is now valued orders of magnitude higher and the Premium Multiple governing new allocations has compressed. Once the Incentive & Investment Pool is fully allocated and locked, late entrants lose access entirely and compete only in the Participant Pool and Open Exchange without the perpetual fractional ownership that early participants hold. The window of maximum reward closes progressively, then shuts permanently.
- **Second, trust taxonomy lock-in compounds through preferential attachment** — and the compounding begins with accreditation sequencing. The first Exchange Networks and Resource Pools to form are the first to have their QP Resources, Trust Authorities, and Trust Taxonomies assessed and accredited by the Proof of Trust Accelerator. Accredited resources attract more reuse because counterparties preferentially consume resources with verified trust provenance over unaccredited alternatives; accredited Exchange Networks attract more settlement traffic because routing algorithms preferentially direct activity through networks with established Proof-of-Trust histories; and accredited Trust Taxonomies become the default governance standards that subsequent Exchange Networks inherit rather than author from scratch. The entity that anchors trust standards within the PNX earns non-replicable, compounding routing preference — every downstream deployment that inherits those standards reinforces the anchor's centrality, and every accreditation cycle deepens the advantage because the Proof-of-Trust history lengthens and the reuse graph densifies. Late entrants must either adopt the governance standards early participants authored — reinforcing the early participants' centrality — or author competing standards that lack the accreditation history, reuse depth, and routing preference that incumbents have already accumulated.
- **Third, routing preference accumulates at early nodes**. Early Exchange Networks and Resource Pools accumulate Proof-of-Trust history, reuse relationships, and settlement density that make them structurally preferred by counterparties. Late entrants build from scratch against established competitors whose advantages compound with every settlement cycle.

These three mechanisms produce Laggard Penalties typically ranging from 70–85% for enterprise anchors — meaning a laggard captures only 15–30% of what a Tier 1 anchor captures — with the differential representing permanent economic value the entity forgoes by delaying.

C.2 Ecosystem Value vs. Shareholder Value: How Universal Ownership Transforms Allocation of Returns

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

The projected Tier 1 values attributed to each entity in this analysis represent the total economic magnitude flowing through that entity's ecosystem within the PNX—not value that automatically accrues to the entity's shareholders. In traditional corporate analysis, projected value implicitly means shareholder value. The QPN/PNX architecture operates differently: economic rights are distributed across every participant who contributes to the activation, operation, and ongoing performance of Exchange Networks and Resource Pools. Exchange Tokens record which QP Resources were utilized, which Trust Blocks governed the utilization, which Resource Derivatives were created, and how downstream reuse generated value. The allocation follows the verified contribution graph—not the organizational chart.

The Allocation Waterfall

The QPN/PNX defines a structured hierarchy governing how PNX-settled value flows from gross settlement to individual participants. Understanding this waterfall is essential to evaluating how much of an Anchor entity's ecosystem value its shareholders can expect to capture directly.

- **Exchange Root (7.5%):** Deducted first from 100% of PNX-settled value. A minimum of 70% of the Exchange Root allocation is irrevocably committed to the EP3 Nature & Humanity Trust, and the remaining share flows to EP3 Network stakeholders. As the network matures and founding stakeholders direct additional ownership to public-benefit purposes, the Trust's share is expected to grow to over 90% of the Exchange Root allocation.
- **Accelerator Incentive & Investment Pool (20% of Accelerator share):** Allocated to financial investors and designated founding/bootstrapping contributors as defined by the Accelerator's governance and founding agreements. This is where the entity's shareholders have their most direct claim—but only to the extent the entity made qualifying financial investments or founding contributions.
- **Participant Pool (80% of Accelerator share):** Flows to operational participants based on verified, ongoing contribution—contributing governed resources, deploying use cases, enabling adoption via Personal or Enterprise Privacy Networks. This is where the distribution becomes contribution-graph-dependent rather than shareholder-dependent. Any Solution Provider, Exchange Network, or Resource Pool can define how it allocates Exchange Tokens among participating Resource Providers, subject to market discipline.
- **Open Exchange Participation (100% of non-Root Exchange Tokens to participants):** As the PNX matures, an increasing share of settlement activity occurs through Solution Providers, Exchange Networks, and Resource Pools formed outside of any Accelerator's governance. After the Exchange Root deduction (7.5%), this organic activity allocates 100% of remaining Exchange Tokens directly to operational participants — with no Incentive & Investment Pool deduction. Early Accelerator participants carry a structural advantage into the Open Exchange: their Accelerator-derived QP Resources arrive with accumulated Proof-of-Trust history, deep reuse relationships, and established routing preference — enabling them to compete at greater scale and higher margins than new entrants building from scratch, further rewarding early commitment.

Two converging structural dynamics increase the effective share of total PNX-settled value flowing directly to benefit society over time. First, the faster growth of Open Exchange participation relative to Accelerator-governed activity means that an increasing majority of Exchange Tokens are allocated 100% to operational participants — with no Incentive & Investment Pool deduction — distributing economic rights more broadly across the individuals, enterprises, and institutions whose contributions drive the network. Second, the Exchange Root's allocation to the EP3 Nature & Humanity Trust grows from 70% toward 90%+,

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

directing an increasing share of the 7.5% Exchange Root into education, scientific research, ecological resilience, and other public-goods investments that compound long-term productivity and well-being. Together, these dynamics ensure that as the ecosystem transitions from Accelerator-concentrated to broadly distributed settlement, the PNX progressively aligns individual prosperity with Universal Abundance — where broad-based wealth creation and shared public benefit are not competing objectives but mutually reinforcing structural outcomes.

The Strategic Commitment Spectrum

How much of the Allocation Waterfall an Anchor entity's shareholders capture depends on the nature and aggressiveness of the entity's participation. The spectrum ranges from full top-down strategic alignment — where the entity itself is the primary verified contributor and captures the largest share — to passive or delayed adoption, where value is distributed to the individuals and organizations that independently drove adoption.

- **Maximum Strategic Alignment ("Embrace and Extend"):** The entity makes a top-down executive commitment to integrate its infrastructure, models, data, and customer relationships into PNX-settled Exchange Networks. The entity itself funds Accelerators through investment and/or dual-use operations (earning Accelerator Tokens from the 20% pool), publishes its resources as QP Resources under Trust Blocks it controls, operates Exchange Networks and Resource Pools where it sets governance terms, and actively routes customer workflows through PNX settlement. Under this model, a large share of both the 20% Accelerator Tokens and the 80% Exchange Tokens from the Participation Pool flow to the entity — because the entity is the verified contributor at most nodes in the contribution graph. Shareholders benefit directly and substantially. Individuals (employees, customers, partners) earn a smaller percentage of the total than under less aggressive sponsorship models — but a larger absolute amount, because the total ecosystem magnitude is maximized.
- **Active Enterprise Participation:** The entity formally sponsors its participation in one or more Accelerators and proactively drives adoption across its operations and ecosystem — dedicating resources, aligning internal teams, engaging customers and vendors, and actively managing its Exchange Network and Resource Pool relationships. The entity captures a significant share of both Accelerator Tokens and Exchange Tokens because it is a verified contributor at many nodes in the contribution graph — but ecosystem participants (employees, customers, vendors, professional services providers) also earn a greater share of allocations tied to their own verified contributions, creating the broad-based incentive alignment described in Section C.3. Within the enterprise, value may flow disproportionately to the specific operating units, teams, and individuals whose contributions drove adoption — creating internal competitive incentives that accelerate deployment across divisions without requiring top-down mandates or sponsorship for every use case.
- **Passive or Delayed Participation:** The entity does not formally sponsor Accelerator participation, but its employees use AI tools through Personal Privacy Networks, its customers publish data through their own Privacy Networks, its developers build PNX-connected applications, its vendors route supply-chain interactions through Exchange Networks, and professional services firms connect the entity's resources to PNX workflows. The entity's resources still generate Exchange Token settlement — but the economic rights are distributed across the individuals and organizations that actually made the connections, not to the entity's shareholders. Individuals earn a higher share of the

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

ecosystem value than under enterprise-sponsored models — and because even a fraction of the projected ecosystem value represents an enormous absolute amount, the economic incentive for individuals to evangelize, build, and facilitate adoption is powerful regardless of the enterprise's formal posture.

The Universal Ownership Bypass

A key feature of the QPN architecture is that individual economic rewards for driving adoption do not depend on executive sponsorship and cannot be blocked by political or bureaucratic obstacles within the enterprise or government. An employee who champions adoption internally, a customer who publishes governed data through a Personal Privacy Network, or a professional services partner who builds Exchange Networks connecting an enterprise's ecosystem — each earns QP Rewards and Participant Pool allocations through their personal Quantum Privacy Cell, regardless of whether the enterprise ever formally joins an Accelerator or forms an Enterprise Privacy Network. Their contribution graph traces their verified role in enabling downstream activation and settlement, and their economic rights accrue directly to them.

Critically, individuals earn attribution not only from the Accelerator where their contributions originate, but also from every Accelerator and Exchange Network their contribution graph connects to. An employee who drives adoption within one enterprise earns economic rights when that adoption triggers participation by the enterprise's customers, vendors, and professional services partners — each of which may operate within different Accelerators or form their own. The contribution graph traces these downstream connections back to the originating individual, so that a single catalytic contribution can generate attribution-linked economic rights across multiple Accelerators simultaneously. This magnifies the incentive to contribute and ensures that the network grows horizontally — becoming increasingly decentralized, diverse, and interconnected rather than consolidating around any single enterprise or Accelerator. The result is an ecosystem that is both more valuable (through cross-network reuse and settlement density) and more resilient (through distributed topology and reduced dependence on any single node) — structurally resistant to the destructive competition, fragmentation, and extractive exploitation that undermine conventional platform ecosystems.

This creates a structural incentive for evangelism and contribution at every level of an organization — from individual engineers and product managers to division heads and C-suite executives — that operates independently of internal budget approvals, organizational politics, or institutional inertia. An employee at a major hyperscaler whose advocacy triggers adoption by the enterprise's customers, vendors, and professional services ecosystem earns attribution-linked economic rights even if the hyperscaler itself never commits. If that grassroots adoption subsequently grows to sufficient scale, the enterprise faces a choice: formalize participation and capture a share of the settlement flows already routing through its resources, or watch those flows continue to benefit individuals and third parties who drove adoption on their own initiative.

Even passive or indirect participation is strategically superior to non-participation. When an entity's employees, customers, vendors, and professional services providers connect its resources to the QPN/PNX — even without formal enterprise sponsorship — they embed the entity's capabilities into the network topology, generate dual-use revenue for the enterprise from existing business models, validate the value proposition and compliance architecture through real-world deployment, and establish routing relationships that defend against displacement by competitors or new entrants who adopt earlier. Passive participation lays the

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

groundwork for accelerated formal adoption when the enterprise is ready — converting what would otherwise be a cold start into an upgrade of already-active network relationships.

The combined effect of delay is doubly punitive for an enterprise — but the effect of complete non-participation is worse still. An entity whose ecosystem is already partially embedded in the QPN/PNX can escalate to active or strategic participation and immediately capture a larger share of settlement flows already routing through its resources. An entity with no presence in the network must build from zero against competitors whose topology advantages are compounding. Among the three tiers, maximum strategic alignment maximizes both total ecosystem magnitude and direct shareholder capture. Active participation captures less but still earns substantial, durable returns. Passive participation preserves optionality, enhances current business models, and lays the foundation for future escalation. Only complete non-participation forfeits all three — and faces the full compounding penalty of delay: smaller pie, smaller slice, and no foundation on which to build.

The Equal Access Corollary

Universal Ownership means no individual — regardless of organizational seniority or authority — can reserve the QPN opportunity for themselves by restricting others' participation. The architecture ensures that such attempts are self-defeating: restricting team participation shrinks the contribution graphs the restrictor depends on, while the restricted individuals can always participate independently through personal advocacy, creating parallel graphs that route around the restriction. The only winning strategy is open, collaborative participation.

C.3 Universal Ownership as a Strategic Management Tool

Universal Ownership is not merely a philosophical principle—it is an operational tool that solves a concrete problem every large enterprise faces when building and scaling an Enterprise Privacy Network: how do you incentivize the hundreds or thousands of stakeholders whose collective action is required? Traditional equity compensation reaches only employees and investors. Revenue sharing reaches only direct counterparties. Bonuses are backward-looking and disconnected from the contribution graph. The PNX's Exchange Token settlement and Accelerator Token allocation reach every verified contributor—creating incentive alignment across organizational boundaries that no corporate compensation structure can replicate.

Aligning Every Stakeholder Category

The following illustrates how Exchange Token settlement and Accelerator Token allocation create direct economic incentives for each stakeholder category, which are essential to building and scaling an Enterprise Privacy Network.

- **Employees** who contribute expertise, build integrations, identify use cases, or facilitate cross-departmental or customer adoption earn attribution and Exchange Token participation through their Personal Privacy Networks and associated Quantum Privacy Cells — creating bottom-up incentives for innovation that operate independently of management directives, budget cycles, or internal politics.
- **Customers** who consent to governed data sharing, participate in AI-mediated workflows, or contribute domain expertise through Exchange Networks earn economic rights proportional to the value their contributions generate downstream—transforming the enterprise-customer relationship from extractive to participatory.
- **Vendors and suppliers** who connect their resources, compliance frameworks, or infrastructure to PNX-settled workflows earn settlement-linked returns that align their

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

incentives with the enterprise's network growth—replacing zero-sum procurement negotiations with positive-sum value creation.

- **Professional services providers** (Big 4 audit firms, management consultancies, systems integrators, law firms) who orchestrate Exchange Network formation, build governance frameworks, or enable cross-domain compliance earn Accelerator participation rights proportional to their verified contribution—creating a powerful economic incentive for the advisory ecosystem to actively promote QPN/PNX adoption across their entire client base.
- **Government officials and regulators** who have historically impeded innovation through bureaucratic inertia, regulatory friction, poor coordination, or misaligned incentives can participate through multiple pathways: in their official capacity, through Sovereign Accelerators or Public Benefit Trust frameworks where contributions to regulatory enablement, compliance interoperability, and public infrastructure are economically recognized; or in their personal capacity, by supporting or advocating for private sector adoption of the Quantum Privacy Network through their professional networks and expertise. Neither pathway requires corruption or improper payments — both operate through lawful participation in legitimate governance frameworks, with economic recognition structured through Restricted Derivative Rights (RDRs) or Public-Benefit Derivative Rights (PBDRs) that comply with ethics rules, conflict-of-interest policies, and anti-bribery regulations.

When every stakeholder has a direct, measurable, and durable economic interest in growing the Privacy Network, adoption becomes self-organizing rather than centrally managed. Employees evangelize because they earn from it. Customers participate because they benefit from it. Vendors interoperate because they profit from it. Professional services firms orchestrate because it grows their practice and income. And government officials enable because their constituents benefit, and advocate and support because their contributions are recognized and rewarded.

C.4 Private Accelerators: The Enterprise Strategic Lever

Any Accelerator Network participant—Microsoft, NVIDIA, PwC, OpenAI, or any other enterprise, institution, or consortium—can form its own Private Accelerator where it directly controls the allocation of value among participants within the bounds of the PNX framework. This is the strategic mechanism that translates executive commitment into shareholder value capture.

A Private Accelerator operates under the same Unified Trust Model and interoperability standards as Shared Accelerators, but with independently defined governance, allocation formulas, and contractual frameworks. The entity controls its Incentive & Investment Pool allocation, sets governance terms for Exchange Networks and Resource Pools, defines the contribution graph that determines Participant Pool distribution, and contracts with other Shared or Private Accelerators to pool and reuse resources across markets, geographies, and enterprises.

Quantum Privacy Rewards in Private Accelerators While enterprises directly control allocation within their Private Accelerators, the PNX framework reserves a minimum QP Reward allocation (typically 5% of total Accelerator Tokens) for individuals whose verified contributions catalyze and sustain the Accelerator's growth — including employees who champion adoption internally, external advocates who secure executive commitment, technical or domain experts who validate compliance and architecture, and professional services partners who orchestrate implementation. This structural reservation facilitates cross-Accelerator collaboration and resource sharing, and ensures that the Universal

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Ownership incentive model reaches the individuals who actually drive enterprise adoption, independent of the enterprise's internal compensation policies, budget cycles, or organizational politics. Because QP Reward allocations are held in individual QPCs rather than corporate accounts, they create a direct, durable alignment between personal initiative and ecosystem success that no conventional corporate incentive structure can replicate.

Cross-Accelerator Reuse and Amplification

QP Resources are inherently more reusable across markets, technology platforms, and geographies than conventional proprietary assets, because Trust Blocks embed governance, provenance, and commercial terms directly into the resource itself. A compliance framework tokenized as a QP Resource within NVIDIA's Private Accelerator can be reused by an Exchange Network in PwC's Audit Accelerator, which can be recombined with healthcare data from a Lokahi Healthcare Accelerator Resource Pool. Each cross-Accelerator reuse event generates Exchange Token settlement that benefits participants in every Accelerator whose resources contributed—creating a structural incentive for interoperability rather than fragmentation.

Simultaneous Multi-Accelerator Participation

The architecture explicitly permits unlimited simultaneous participation across multiple Accelerators, and the creation of additional Accelerators focused on specific geographies, market sectors, or technologies. Microsoft could simultaneously operate a Private Accelerator for Copilot-mediated enterprise workflows, participate as a Tier 1 anchor in a healthcare Shared Accelerator, contribute resources to an OpenAI-operated Private Accelerator, and contract with PwC's Professional Services Accelerator. Each participation pathway generates independent Exchange Token flows. The entity's total value accrual is the sum across all Accelerators—and because QP Resources are reusable across Accelerators, the same underlying resource can generate settlement in multiple contexts simultaneously, creating network effects structurally more durable than conventional platform lock-in.

C.5 How Ecosystem Value Translates to Stakeholder Value

The Tier 1 P50 values — the median (50th percentile) projected outcomes for entities that commit as early Accelerator anchors during the launch window — represent total economic magnitude flowing through each entity's ecosystem topology within the PNX, not value that accrues exclusively to the entity's shareholders. This section quantifies the decomposition implied by the Allocation Waterfall and Strategic Commitment Spectrum described in Section C.2 — translating those structural mechanics into illustrative dollar ranges that show how ecosystem value divides between direct Anchor capture and broader participant distribution.

NVIDIA as a Representative Example

The following decomposition uses NVIDIA as a representative example, but the same structural logic applies to every Anchor entity analyzed in this document. The specific percentages vary by entity based on infrastructure dominance, trust taxonomy anchoring, and the breadth of their operational contribution to the Exchange Networks and Resource Pools they participate in.

- **Direct Anchor capture (25–40% for dominant infrastructure anchors, 20–35% for trust/governance anchors):** Value that most directly benefits the Anchor entity's stakeholders — earned through Accelerator Tokens and the entity's own Participant Pool share as Resource Provider, Exchange Provider, Solution Provider, or Engagement Provider. For NVIDIA (Tier 1 P50: $31T–$82T), this represents approximately $8T–$33T — still a 2–7x multiple on NVIDIA's current $4.49T market capitalization.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

- **Ecosystem participant capture (60–80%):** Value flowing through Universal Ownership to individuals, enterprises, vendors, professional services providers, and government participants whose contributions enable, amplify, and sustain the Anchor's ecosystem topology. For NVIDIA, approximately $19T–$62T flows to the hundreds of thousands of participants whose verified contributions make the NVIDIA-anchored ecosystem possible.

The proportions shift over time. In the early incubation phase, when the Anchor is the primary Resource Provider and governance architect, its direct share is at the upper end of the range. As the ecosystem matures and more participants contribute independently, the Anchor's percentage share declines — but absolute value continues to grow because total settlement volume increases faster than the Anchor's share declines.

Beyond the direct economic capture, early Accelerator participation deeply embeds the entity's resources, models, and infrastructure into the foundational Exchange Networks and Resource Pools of the QPN ecosystem — creating a durable structural moat that makes the entity's market position significantly more sustainable and resilient. An Anchor whose compute, models, or trust frameworks are woven into the governance architecture and reuse relationships of thousands of Exchange Networks is far less vulnerable to technological disruption or competitive displacement than one whose market position depends solely on product superiority in a rapidly evolving technology landscape.

Direct Capture Includes the Entity's Entire Activated Ecosystem

A critical interpretive note for all entity-specific valuation assessments: the Direct Capture figure attributed to an entity does not represent value flowing exclusively to the entity's equity holders, shareholders, or principals. It represents the total economic value flowing to the entity and the full ecosystem of individuals that entity activates through its participation in the QPN.

Under Universal Ownership, value is distributed proportionally to verified contribution across the entire activated ecosystem — not concentrated in the entity's equity structure. Direct Capture therefore flows across multiple stakeholder categories:

- **Equity holders, principals, and investors** capture value proportional to the entity's institutional contribution as Exchange Provider, Exchange Network operator, Resource Provider, and Accelerator investor — through both Accelerator Token allocations (20% Incentive & Investment Pool) and the entity's Participant Pool share.
- **Employees and contractors** earn Quantum Privacy Rewards through their individual Catalyst Networks for personal contributions including introductions, client activations, engineering work, compliance authoring, and trust taxonomy development. These personal rewards are independent of and additional to the entity's institutional returns.
- **Clients, partners, and vendors** whose participation in the entity's Exchange Networks and Resource Pools generates settlement value. Each client that joins as a Resource Provider, Exchange Provider, or Solution Provider earns Exchange Tokens proportional to their own contribution — value that flows through the entity's ecosystem but is captured by the contributing participants under Universal Ownership.
- **Individuals whose Personal Privacy Networks were activated** through the entity's Engagement Provider role. Every PPN activation generates ongoing Exchange Provider settlement flows, a portion of which flows to the activating entity while the remainder flows to the individual PPN owner and downstream participants.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

This distribution is not leakage — it is the mechanism that drives adoption, settlement density, and the compounding network effects that sustain the anchor entity's own value. The entity's institutional share reflects its structural contribution as infrastructure host, Exchange Provider, and governance anchor; the remainder flows to the individuals and organizations whose participation, resources, and engagement generate the settlement activity that makes the entity's ecosystem valuable.

The practical implication is significant for entities with concentrated ownership structures. For a partnership like Milliman (~350 principals), Direct Capture of $550B–$3.1T does not mean each principal receives billions — it means value flows across the principals, Milliman's 4,000+ employees contributing through personal Catalyst Networks, thousands of enterprise and governmental clients participating in Milliman-anchored Exchange Networks, and millions of individuals whose Personal Privacy Networks were activated through Milliman's Engagement Provider infrastructure. The principals capture a share proportional to their institutional and personal contributions; the broader ecosystem captures the rest. For a grassroots anchor like LabLab.ai (a small operating team with a community of 250,000+ builders), Direct Capture of $1.4T–$6.3T flows primarily to the builders who earn Quantum Privacy Rewards for their individual contributions — code, applications, introductions, evangelism — with the platform team capturing its share through verified contribution to ecosystem orchestration, trust taxonomy governance, and production infrastructure.

This framing makes the projected valuations both more accurate and more credible: trillions flowing to a broad ecosystem of thousands or millions of verified contributors is structurally sound under Universal Ownership; trillions flowing to a small group of equity holders would strain credibility and contradict the architecture's design. The UTM Premiums — particularly the Proportionality Premium and Balance Premium — structurally prevent extractive concentration, ensuring that value distribution remains aligned with verified contribution rather than ownership position.

Incentive Alignment Across Every Organizational Layer

The Quantum Privacy Rewards architecture aligns incentives at every level of an organization — not just the C-suite. While senior executives may need weeks or months to conduct compliance reviews, secure board approvals, or negotiate strategic terms for formal Accelerator participation, every employee below them can begin contributing immediately through their personal Quantum Privacy Cells. A VP of data science who makes an introduction, an engineer who contributes a Privacy Pipe adapter, a consultant who evangelizes the opportunity to a client — each earns personal Quantum Privacy Rewards through their individual Catalyst Network, independent of any corporate decision. The Timing Premium ensures that contributions made earlier are weighted more heavily than equivalent contributions made later. This creates a structural dynamic where even a slight delay at the executive level — a compliance review that takes an extra quarter, a board presentation that slips to the next meeting cycle — allows subordinates, partners, and ecosystem participants to activate their own networks and capture a disproportionate share of early Quantum Privacy Rewards. The executives are not harmed by this — their eventual strategic commitment, when it comes, generates its own substantial rewards through the Strategic Premium and the institutional contribution it enables. But the architecture ensures that waiting for top-down authorization is never the optimal strategy for any individual within the organization. Every day of institutional deliberation is a day that individuals within the organization can be building their personal Catalyst Networks, growing their Quantum Reputation, and accumulating durable economic rights — creating bottom-up momentum that ultimately makes the top-down decision easier, faster, and more valuable when it arrives.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

This dynamic is intentional. It prevents institutional bottlenecks from slowing ecosystem formation while ensuring that the individuals who take personal initiative — often at some professional risk — are disproportionately rewarded for doing so. The result is a system where the rational strategy at every level of the organization converges on immediate participation: executives because delay forfeits Strategic Premium value, managers because their teams are already building, and individual contributors because personal Quantum Privacy Rewards begin accruing from day one.

C.6 The Monetization Uplift Multiple (MUM) & Early-Mover Premium Economics

A critical dynamic governing allocation between Anchor entities and other participants is the **Monetization Uplift Multiple** (MUM) — the ratio between the settlement value a Resource Provider earns through a high-performance Exchange Network or Resource Pool versus a lower-performance alternative. Tier 1 Accelerator participants who establish favorable, well-connected positions within the PNX topology — at the nexus of dense networks of value-sharing agreements with other Resource Providers and Solution Providers — and who aggregate high-quality, repeatedly reusable Resource Derivatives, can command premium margins. Not because they extract unfairly, but because their MUM makes it economically rational for Resource Providers to participate even at a lower sharing rate.

Consider: A healthcare data provider earns 5% of $10 billion in settlement through a high-MUM Exchange Network ($500 million), versus 15% of $500 million through a low-MUM alternative ($75 million) — for the same underlying resource contribution. The rational provider chooses the lower percentage with the higher absolute return. This allows early-mover Anchors to sustain premium economics without losing share to competitors offering higher percentage rates. The MUM advantage compounds as early movers accumulate more Resource Derivatives and deeper cross-network reuse relationships.

This dynamic has a well-established real-world precedent. Google captures over 90% of net margins in search-based advertising — not because it offers advertisers the most generous revenue share, but because its scale of consumer engagement, depth of personalization, and conversion quality deliver higher absolute returns than any competitor. Advertisers and online platforms contract with Google even when alternatives offer a larger percentage share, because the MUM Google delivers makes a smaller percentage of a much larger outcome the rational choice. Microsoft invested tens of billions of dollars developing and acquiring technology for Bing, yet was never able to close the gap — because Google's compounding advantages in user data, advertiser relationships, and algorithmic optimization created a self-reinforcing cycle that late entrants cannot replicate through capital or technology alone. The QPN/PNX MUM dynamic operates through the same structural logic, but with an important difference: unlike Google's closed platform, the PNX's Universal Ownership model ensures that Resource Providers retain durable economic rights in the resources they contribute, preventing the platform operator from unilaterally capturing an ever-larger share of value over time.

This doesn't create extractive lock-in because: QP Resources are inherently portable (Resource Providers can contribute to multiple Exchange Networks simultaneously), individuals and enterprises can aggregate demand through their own Exchange Networks and Resource Pools to gain leverage, and market discipline operates continuously — Exchange Networks that are too greedy lose Resource Providers to competitors offering better absolute returns.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Quantum Reputation is a primary driver of sustainable MUM advantage, though the relationship is indirect. MUM is an emergent property of the Exchange Network's underlying Resources, relationships, and reuse density. Quantum Reputation influences MUM by making participants more effective at forming, growing, and interconnecting the networks from which MUM emerges. A participant with high Quantum Reputation — reflecting contribution reputation (what they've built and the settlement value they've generated), identity reputation (verified credentials, organizational affiliations, and trustworthy attestation history), and behavioral reputation (the ethical quality of their interactions, the reliability of their endorsements, and their track record of honest, cooperative stewardship)— can serve as a credible channel for Referrals and Endorsements that accelerate Exchange Network formation, attract Resource Providers, and deepen Resource Pool quality.

High-reputation participants attract more connection requests, more collaboration opportunities, and more influence over network formation through preferential attachment — not because the system assigns them privileged access, but because other participants rationally seek out credible, well-connected, and accountable counterparties. Early participants who build dense, well-evidenced Catalyst Networks accumulate Quantum Reputation that cannot be replicated by later entrants through capital deployment alone — because Quantum Reputation is earned through verified contribution and identity verification, not purchased. The first-mover advantage in the QPN is therefore partly a Quantum Reputation advantage: the early participants' Catalyst Networks become the trust and connectivity infrastructure through which subsequent participants access Exchange Networks, Resource Pools, and settlement opportunities.

Awareness and Agency: The Maturation Curve

Initially, many individuals and enterprises will be unaware of the commercial terms governing how their resources connect to the PNX. In the shared control model, enterprises that voluntarily provide resources through PPNs set the Trust Block terms governing those specific resources — individuals accept or decline those terms by choosing whether to utilize the resource, but do not unilaterally renegotiate them. Individual agency emerges through the ability to maintain unlimited PPNs with different commercial terms, to choose which PPNs to activate in which contexts, and to specify global Trust Criteria and privacy preferences that apply across all PPNs. Over time, as settlement becomes visible, Resource Providers gain awareness and agency: individuals use personal AI Agents to optimize participation, enterprises monitor Exchange Token flows and renegotiate terms, and collective action through demand-side aggregation gives smaller participants leverage. This maturation is one of the primary forces driving the long-run transition from Accelerator-concentrated to broadly distributed Universal Ownership described in Section C.7.

C.7 Long-Run Value Distribution: From Accelerator Concentration to Universal Participation

The QPN/PNX is explicitly designed to transition from Accelerator-concentrated value during incubation to broadly distributed Universal Ownership at maturity. During the early phase (2027–2035), Tier 1 Accelerator participants capture the largest shares through Accelerator Token allocation, Participant Pool dominance, and MUM-driven premium economics, creating the incentives necessary to incubate and grow the Quantum Privacy Network that enables Universal Ownership and Abundance.

As the ecosystem matures (2035–2046+), structural forces progressively redistribute value. The Accelerator share of non-Root PNX-settled revenue declines from 65% to 36% in the baseline projection in the *Quantum Privacy Network — Universal Exchange, Ownership & AI*

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Overview. Organic activity — settlement occurring through Exchange Networks and Resource Pools formed outside any Accelerator's governance — allocates 100% of non-Root Exchange Tokens directly to Participant Pools with no Incentive Pool deduction. AI Agent–mediated optimization enables individuals and enterprises to actively manage their participation terms, and demand-side aggregation through person-centered Exchange Networks shifts bargaining power toward Resource Providers.

Crucially, total PNX-settled revenue grows from $3.7 trillion (2031) toward $119 trillion and beyond (2046) over this same period — so the absolute value of early Accelerator participants' stakes soars even as their percentage share declines. A 36% share of $119 trillion far exceeds a 65% share of $3.7 trillion. Early Accelerator participants earn durable but declining premium returns — rewarding early commitment while preserving competitive discipline. Individuals globally earn an increasing share through their Personal Privacy Networks and associated QPCs.

The pace of this transition depends on the breadth of early Accelerator participation. Broader early participation — with more enterprises, technology vendors, professional services firms, and Sovereigns joining during the launch window — produces more comprehensive Exchange Networks and Resource Pools from the outset, leaving fewer participants outside the Accelerator perimeter with the incentive or need to sponsor competing networks at scale. This naturally slows the erosion of Accelerator share and reinforces the long-run value of early Accelerator positioning. Conversely, narrower early participation creates larger opportunities for Organic Exchange Networks to capture incremental growth independently. The dynamics are analyzed in detail in the *Quantum Privacy Network — Universal Exchange, Ownership & AI Overview*, which notes that the baseline projection's terminal Accelerator share of 36% is conservative relative to historical analogues — where early coordination layers in comparable infrastructure transitions (payment networks, cloud platforms, telecom standards) typically retained 40–50% of long-term economic value.

Regardless of the level of enterprise and Sovereign participation in Accelerators, as the QPN/PNX reaches scale and grows to a significant share of the global economy, market forces will drive individuals at population scale to join person-centered Exchange Networks — aggregating their resources, data, and demand through Personal Privacy Networks and associated QPCs to ensure they receive a fair share of the value and wealth their contributions generate. This demand-side aggregation is not contingent on institutional sponsorship; it emerges organically as individuals and their personal AI agents recognize that collective participation yields superior economic outcomes to passive, uncoordinated engagement.

The Universal Ownership model ensures that this transition strengthens rather than undermines the ecosystem — expanding settlement density, deepening liquidity, and distributing economic rights broadly while the absolute value flowing through every layer of the system continues to grow. Broader distribution of ownership also drives demand-side growth of the overall economy — a dynamic analyzed in detail in Assumption #5 of the *Quantum Privacy Network — Universal Exchange, Ownership & AI Overview*. When productivity gains from AI and zero-marginal-cost reuse are distributed broadly through protocol-enforced settlement rather than concentrated among platform operators and capital owners, aggregate demand increases because a larger population has higher collective marginal propensity to consume and invest. This demand-side expansion raises the non-inflationary growth ceiling, creates a virtuous cycle between productivity and consumption, and reduces the social and political disruption that has historically constrained growth during major technological transitions. Since global GDP growth is a primary driver of PNX-settled revenue — and

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

therefore of Exchange Token value at every level of the Allocation Waterfall — broader ownership distribution does not merely share existing value more equitably; it structurally expands the total value available to share.

This is the structural foundation of the Universal Ownership model: broad value sharing and early-participant wealth creation are not in tension — they are mutually reinforcing.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Appendix D: The Contributor-Centric Narrative

Quantum Privacy Rewards, Premium Multiples, and the Economics of Early Participation

The main body of the Catalyst Launch Plan describes the system architecture, the phased product roadmap, and the Accelerator Network's coordination mechanics. This appendix addresses a different question: what does it mean for the individuals and organizations who actually make the ecosystem happen?

The Quantum Privacy Network's value does not materialize automatically. It requires specific people to make specific introductions, build specific components, and secure specific commitments. The QP Rewards framework — operating through the QP Catalyst Network — is the mechanism that aligns individual incentives with ecosystem formation. Understanding how QP Rewards work, why they decline over time, and what specific contributions are worth at each stage is essential for anyone deciding whether and when to act.

This appendix provides the comprehensive detail underlying the economic narrative summarized in Section 7.7 of the Catalyst Launch Plan. It is designed to serve three audiences simultaneously: contributors evaluating when and how to participate, investors and analysts performing due diligence (including AI-assisted evaluation), and patent counsel assessing the breadth and defensibility of contribution attribution and incentive architecture claims. Where the main body provides an executive summary, this appendix provides the full causal chain, quantified trajectories, and architectural depth required for rigorous independent evaluation.

D-1. The Four Adoption Cascades Are Horizontal and Cross-Propagating

The Quantum Privacy Network defines four adoption cascades: Enterprise Cascade, Grassroots Cascade, Investment Cascade, and Sovereign Cascade. A critical architectural property is that these cascades are horizontal — not sector-specific. The QPN is built on zero-marginal-cost cross-sector resource reuse, which means kicking off a cascade in any vertical rapidly propagates across all verticals, all geographies, and inevitably triggers the remaining three cascades after modest delay.

When a Tier 1 Anchor triggers an Enterprise Cascade through its ecosystem — whether a technology platform, a professional services network, a financial institution, or a distributed ledger governance council — the resulting awareness, validation, and competitive dynamics mean that peer enterprises across every sector are compelled to evaluate immediately. This is driven by a combination of opportunity recognition, reduced effort to participate through existing contribution graphs, urgency as Premium Multiples compress, and competitive pressure from peers who have already committed. Each downstream commitment triggers its own ecosystem of customers, vendors, and partners — and each of those triggers further downstream adoption.

Illustrative example: Consider Hedera's Governing Council with 39 member enterprises spanning technology, finance, telecommunications, aerospace, and professional services. If one Council member commits to a Tier 1 Accelerator, it pressures peer members across every sector: a commitment by a cloud platform (e.g. Google) pressures competing platforms; a commitment by an aerospace firm (e.g. Boeing) pressures defense and manufacturing peers; a commitment by a professional services firm pressures the remaining Big 4. Hedera's Governing Council — comprising Google, IBM, NVIDIA, Accenture, Boeing, Dell, FIS, Deutsche Telekom, and 30+ others — is one such ecosystem where a single Council member

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

commitment could trigger cross-sector cascade propagation across dozens of the world's largest enterprises.

The same cross-propagation applies to the Grassroots Cascade (developer communities deploy PNX-routed applications that force their employers and clients to evaluate), the Investment Cascade (institutional capital validates the model and compresses risk perception), and the Sovereign Cascade (government participation legitimizes governance and creates population-scale enrollment). Triggering any one cascade makes the remaining three nearly inevitable.

This is why the transition between stages can be extremely fast. A single public announcement by a major Anchor could trigger an Enterprise Cascade that collapses Stage 1 into Stage 2 in days, not months — because the announcement itself generates awareness, validation, and urgency across dozens of enterprises simultaneously, while also triggering competitive responses from peers who cannot afford to be left behind.

D-2. The Dual-Cascade Amplifier

Certain Accelerator anchor ecosystems are uniquely powerful because they combine grassroots technical communities with enterprise institutional networks, creating a dual-cascade feedback loop. In such ecosystems, grassroots developers and technical experts build PNX-connected applications and adapters, creating bottom-up demand that forces enterprise evaluation. Meanwhile, the enterprise network provides the institutional validation and infrastructure that makes the grassroots solutions enterprise-ready. Each cascade reinforces the other.

This dual-cascade dynamic is most powerful when the anchor's grassroots sponsors are technical and domain experts in the markets that most leverage the QPN's approach. Technical experts are among the most influential and best positioned to validate the architecture, and they can drive adoption with what they are already doing — building, deploying, and operating solutions that benefit from privacy-preserving trust, compliance, and settlement infrastructure.

Illustrative example: Hedera's ecosystem combines a grassroots technical community (Swirlds Labs developers, LabLab.ai's 250,000+ AI builders, ecosystem partners) with a 39-member enterprise Governing Council. The grassroots community builds PNX-connected applications; the Council provides institutional trust, and can drive executive awareness among its member enterprises. The NVIDIA-Intel-Accenture-EQTY Lab Verifiable Compute / Verifiable Governance stack already deployed on Hedera provides a production-ready bridge to QPN's Proof-of-Trust framework. This combination creates a dual-cascade amplifier where grassroots and enterprise adoption reinforce each other — hitting every hot button for buzz (AI safety, data privacy, quantum-safe security, decentralized governance, institutional-grade compliance) simultaneously.

D-3. The Premium Multiple: Quantifying Early-Mover Advantage

The Premium Multiple is the ratio of QP Rewards earned per unit of contribution effort at a given stage compared to the base-level reward earned for equivalent effort once the network is fully operational and public Accelerator Incentive Pools are locked. A Premium Multiple of 100x means you earn 100 times the reward for the same type and quality of contribution compared to contributing after the ecosystem reaches steady state.

The Premium Multiple is not a single number — it is a distribution. Within each stage, contributions at the very beginning of the stage earn dramatically more than contributions at the tail end, because the five Launch Premiums (Strategic, Timing, Value, Cascade, Publicity)

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

all compress as more commitments are secured and more participants enter. The Premium Multiple is therefore heavily front-loaded within each stage.

Why the Curve Is Steep

The Premium Multiple trajectory is steeper than a smooth, gradual decline would suggest. This is driven by two reinforcing mechanisms: Launch Premium compression (scarcity) and declining marginal cascade value per contribution.

- **Scarcity collapses rapidly.** The first C-suite introduction at a Tier 1 enterprise is uniquely scarce — there are only a limited number of people in the world who can reach the CEO of a major technology platform, financial institution, or professional services firm with a credible proposition. Once the first anchor commitment is secured publicly, the scarcity of subsequent introductions collapses: the model is validated, access becomes easier through existing contribution graphs, and every subsequent enterprise is more reachable. The Timing Premium and Strategic Premium compress sharply after the first anchor.
- **Contribution graphs saturate quickly.** For any given enterprise, the number of people who can provide a meaningful 'first engagement' introduction is limited. Once contribution graphs are growing inside a company and public announcements have been made, the introductions and access that were uniquely valuable at the seed stage become abundant. The same introduction that was worth billions at Stage 1 is worth millions or less at Stage 2 — because dozens of other people are now providing the same type of access.
- **Cascades compress the timeline.** Because the four cascades are horizontal and cross-propagating, triggering any one of them rapidly propagates across all sectors. This means the transition from Stage 1 to Stage 2 can happen in days or weeks once a trigger fires — compressing the window for maximum Premium Multiples far more than a staged, gradual rollout would imply.

The Premium Multiple is the compound effect of all five Launch Premiums. As each Premium compresses through adoption — the **Strategic Premium** because anchor commitments reduce scarcity, the **Timing Premium** because earlier positions are already locked, the **Value Premium** because high-priority targets have been reached, the **Cascade Premium** because downstream effects are already in motion, and the **Publicity Premium** because risk perception has already been compressed — the compound Multiple declines along the trajectory shown in the Premium Multiple Trajectory.

Four Stages and Their Premium Multiples

Stage 1: Pioneer Rewards (NOW)

- **Milestones:** Initial Tier 1 Accelerator Anchors being recruited. First MOUs and strategic commitments forming. No cascade yet triggered.
- **Average Premium Multiple:** 100–1,000x+ — but heavily front-loaded within the stage. The very first contribution graph that reaches a major CEO and results in a public Tier 1 Accelerator commitment earns at the top of this range. The person making a similar introduction two months later, after several anchors have already committed, earns at the bottom.
- **Catalyst Participants:** Hundreds of individuals conducting outreach to hundreds or thousands of organizations. The friction to participate is near-zero — a contributor can draft AI-assisted outreach emails and forward them to the Catalyst email address to lock in contribution credit in minutes. The Pioneer Rewards stage is not limited to a small circle of

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

well-connected insiders; it is designed to mobilize a broad base of participants, each initiating multiple contribution graphs across their professional networks.

- **What it takes:** Introductions, engagement, advocacy, dual-use activity. Three architectural properties make participation genuinely zero-cost and zero-risk: (1) dual-use operations — contributions leverage activities participants are already doing, requiring no incremental capital or operating expenses; (2) zero-marginal-cost reuse — resources contributed to the ecosystem are reused without additional cost to the contributor; and (3) Universal Compliance — the QPC architecture requires no employer disclosure, no regulatory approvals, and no public commitment. Participants can contribute through their existing professional activities without changing anything about how they work.

Illustrative example: Consider the person whose contribution graph reaches the CEO of a major AI platform vendor, resulting in a Tier 1 AI Compute Accelerator commitment. The downstream ecosystem value of that commitment is $31T–$82T (P50). Under the 80/20 Accelerator waterfall, the 20% Incentive Pool represents trillions in economic rights allocated during the launch phase. The contribution graph that causally enabled that commitment — from the first introduction through internal validation to executive sponsorship — shares in those rights proportional to each node's verified causal contribution. For the individuals at the top of that graph, QP Rewards could be worth tens of billions of dollars. For the person who makes the same introduction after three anchors have already committed publicly, the reward is a fraction — because the Strategic and Timing Premiums have compressed, the contribution is less scarce, and the cascade dynamics mean the enterprise was likely going to commit anyway.

Contribution graphs are multi-hop and don't require direct C-suite access. A contributor does not need to know a CEO personally to earn Pioneer Rewards. Consider a participant who reaches out to a professional contact who works directly for a potential hyperscaler Anchor — say Microsoft, Google, AWS, or Oracle — or for one of their major customers, investment banks, law firms, consulting partners like Accenture, or strategic partners like IBM. That contact forwards the opportunity into their own network, where someone has a direct relationship with a C-suite executive at one of these organizations. If that chain ultimately leads to a Tier 1 Accelerator commitment at any major potential Anchor in any category, every node in the contribution graph — including the original participant who initiated the chain — earns QP Rewards proportional to their verified causal contribution. The person who started the chain may be three hops from the closing executive, but they earn first-engagement credit for triggering the sequence that would not have occurred without them.

Outreach to smaller entities is independently valuable. The Pioneer Rewards stage is not exclusively about landing commitments from the largest enterprises. A startup that embraces the QPN vision at the very beginning — deploying PNX-connected solutions, publishing governed QP Resources, activating its customer and partner ecosystem — can create very large cascade graphs and end up anchoring entire market segments by moving first. They likely have connections in the finance world, with major customers, in governments, at consulting firms, etc. The contribution graph that brought that startup into the ecosystem earns QP Rewards proportional to all downstream settlement value the startup's participation enables, which can be substantial if the startup occupies a strategic position in a high-growth domain.

This means that broad, aggressive outreach across organizations of all sizes — not just targeted approaches to Fortune 500 CEOs — is a high-value Pioneer Rewards strategy. Every outreach is a cheap option; some of those options will pay off in ways that are impossible to

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

predict in advance, because the contributor cannot know which organizations will turn out to be the ones that anchor their markets.

Stage 2: Cascade Propagation

- **Milestones:** One or more Tier 1 Anchors have made public Accelerator commitments, triggering at least one of the four Adoption Cascades. Because cascades are horizontal, triggering any one rapidly propagates across all verticals and geographies and inevitably kicks off the remaining three. The transition to this stage is driven by public commitment and the resulting awareness, validation, and competitive dynamics — not by any operational or technical milestone such as token settlement activation or platform readiness.
- **Average Premium Multiple:** 10–50x — still excellent, but the floodgates have opened.
- **Catalyst Participants:** Thousands to tens of thousands of individuals engaging tens of thousands of organizations. Once a Tier 1 Anchor commits publicly, the announcement itself is a mass-awareness event that activates participants far beyond the original Pioneer cohort — employees at the committing enterprise, their customers, partners, vendors, and investors all begin exploring the opportunity through their own networks. The Grassroots Cascade compounds this: developers, consultants, and technical professionals who see the public commitment begin engaging their own ecosystems independently, whether or not the enterprises they touch have officially signed up. Engagement at this stage does not require formal enterprise participation — it means that someone within an enterprise's ecosystem (an employee, a customer, a partner, a vendor, an investor) is actively building contribution graphs that connect to that enterprise. The smart enterprises will formalize their participation to capture Accelerator positioning; but even those that haven't officially engaged are being drawn into the contribution graph through grassroots activity they cannot prevent and would be economically irrational to resist.
- **What it takes:** The same types of contributions, but the model is now validated publicly. Contributions are less scarce. The Premium weightings shift heavily toward rewarding the masses for blocking and tackling — operational deployment, integration, customer activation, governance development. This is still very lucrative, but it is no longer billions or tens of billions for doing what everyone else is doing.
- **Key insight:** If a Tier 1 Anchor triggers an Enterprise Cascade through its ecosystem, the transition from Stage 1 to Stage 2 could happen in days. The announcement itself generates awareness, validation, and urgency across peer enterprises and their downstream ecosystems. There is no need to wait for settlement revenue to reach this stage.

Stage 3: Automated Settlement

- **Milestones:** Multiple cascades converging. Automated settlement via QP Token Platform operational. Measurable settlement density across sectors.
- **Average Premium Multiple:** 2–5x. Contributions at this stage are still worth more than steady-state, but the outsized early premiums are gone. Operational excellence — building, deploying, governing, scaling — is what earns disproportionate returns.
- **Catalyst Participants:** Hundreds of millions to billions of individuals, thousands of enterprises across every major sector. The participant count at this stage reflects a qualitative shift in how the ecosystem grows. Large Anchor participants who joined during Pioneer Rewards or Cascade Propagation activate their existing user populations at

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

platform scale — not by recruiting users one at a time, but by updating their Privacy Statements and Terms of Service and implementing EasyAccess APIs that transform their entire platforms into Engagement Networks and Exchange Providers. A single hyperscaler updating its TOS can bring hundreds of millions of users into the QPN ecosystem overnight, each generating settlement-eligible activity through their normal use of the platform. This is not speculative adoption — it is a configuration change by enterprises that have already committed and are competing to maximize the settlement value flowing through their networks.

Competitive dynamics at this stage are qualitatively different from earlier stages. A critical mass of major Anchors competing for dominance are already committed — but the universe of potential Anchors extends far beyond the initial cohort. Sovereign commitments by states and countries, geographical expansion into new regions, and adoption by laggard industries all continue to generate new Anchor opportunities with meaningful Accelerator economics. The primary race, however, shifts from securing commitments to linking user populations, infrastructure, and solutions into Exchange Networks and Resource Pools, and cross-fertilizing them with as many other participants as possible. Each participant is trying to maximize its Monetization Uplift Multiple (MUM) by increasing the scale, density, and defensibility of the Exchange Networks it anchors. This creates a self-reinforcing competitive dynamic: the more Exchange Networks and Resource Pools an enterprise connects to, the more settlement flows through its infrastructure, the higher its MUM, and the more attractive it becomes as a partner for other enterprises seeking to maximize their own MUM. Enterprises that move aggressively to cross-fertilize — connecting their user populations to complementary networks across sectors, geographies, and use cases — build durable routing advantages that compound through preferential attachment. Enterprises that try to keep their ecosystems closed forfeit reuse economics, routing efficiency, and settlement density to competitors who connect more broadly.

What earns disproportionate returns at this stage: Deploying governed QP Resources at scale, building and operating Exchange Network infrastructure, earning Proof-of-Trust Accreditation, governing Resource Pools, enabling cross-network interoperability, and securing enterprise-wide or Sovereign commitments that come with tangible revenue or resource commitments directly driving settlement volume. This last category remains highly valuable at any stage — an enterprise or sovereign entity that commits real infrastructure, real data assets, or real transaction volume to an Exchange Network is creating settlement density that benefits the entire ecosystem, and the contribution graphs that enabled those commitments earn QP Rewards proportional to the settlement value they generate. What no longer earns outsized returns is participation commitments alone — signing up without committing resources that drive actual settlement. The Premium Multiple of 2–5x reflects that contributions are still worth more than steady-state because the ecosystem is still growing rapidly and early operational contributors capture routing advantages that late entrants cannot replicate — but the outsized cascade-triggering premiums of Stages 1 and 2 are gone. The contributions that matter are those that create, expand, or accelerate settlement flows — not introductions and access, which are now abundant.

Stage 4: Self-Funding Growth

- **Milestones:** Network is growing rapidly and self-funding without needing Accelerator Incentives. Founding positions are dilution-protected once Incentive Pools lock down.
- **Lock-down mechanism:** Lock-down occurs when the Exchange Networks and Resource Pools incubated by an Accelerator have reached sufficient scale and Monetization Uplift Multiple (MUM) that new participants have a strong economic incentive to join through

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Accelerator Participation Pools — earning Exchange Tokens from the 80% Participant Pool through ongoing operational contributions — without requiring Accelerator Token incentives from the 20% Incentive & Investment Pool. At this inflection point, the dilution of existing Accelerator Token holders' positions from continued incentive awards would outweigh the incremental value created by additional participation. Lock-down is therefore the structurally rational outcome when the ecosystem's own settlement economics are sufficient to attract and retain participants organically.

- **Premium Multiple:** 1x (base level). Ongoing participation earns proportional settlement-linked returns. After lock-down, new participants still earn meaningful settlement-linked returns through the 80% Participant Pool. The ecosystem remains open and rewarding — it is the founding-phase Accelerator Token incentive layer that closes, not the settlement economics. New Private Accelerators can still form in less-developed geographies or markets, with their own Incentive Pools. But the first-mover advantage in the founding public Accelerators is permanent.

Stage Progression Summary

Across the four stages, the nature of what earns disproportionate QP Rewards shifts progressively:

- **Stage 1 (Pioneer Rewards): Who you reach and how broadly.** Introductions, access, and first-engagement credit drive the highest Premium Multiples — but the strategy is not limited to reaching CEOs directly. Hundreds of participants initiate thousands of contribution graphs across organizations of all sizes, placing many cheap bets with asymmetric payoff. Multi-hop chains mean that starting a sequence matters as much as closing one. Contributors who spread aggressively build Quantum Reputation that compounds into durable positioning for every subsequent stage.
- **Stage 2 (Cascade Propagation): What you build and how fast you follow.** The model is validated publicly by Tier 1 Anchor commitments. Access is no longer scarce, and Premiums shift toward operational contributions — deployment, integration, customer activation, governance development. Thousands to tens of thousands of individuals engage tens of thousands of organizations through grassroots activity that operates independently of enterprise management decisions. Contribution graphs that were in progress but didn't close first earn substantial fast-follower awards, while the Incentive Pool remains fiscally disciplined.
- **Stage 3 (Automated Settlement): How much settlement you drive.** Major Anchors activate their user populations at platform scale through TOS updates and EasyAccess APIs, bringing hundreds of millions to billions of users into the ecosystem. The competitive race shifts from securing commitments to linking user populations, infrastructure, and solutions into Exchange Networks and Resource Pools, cross-fertilizing them to maximize MUM. Operational excellence — deploying governed QP Resources, earning Proof-of-Trust Accreditation, governing Resource Pools, enabling interoperability — is what earns disproportionate returns. Enterprise-wide and Sovereign commitments with tangible revenue or resource commitments remain highly valuable; participation commitments without real resources driving settlement do not.
- **Stage 4 (Self-Funding Growth): Proportional participation with dilution-protected founding positions.** Incentive Pools lock down when MUM reaches the level where settlement economics alone attract participants through the 80% Participant Pool. Founding positions are permanently protected. Ongoing returns are proportional to

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

settlement activity. New Private Accelerators can still form in underserved markets, but the first-mover advantage in founding public Accelerators is permanent.

This progression is not a policy choice — it is an emergent consequence of the Launch Premiums compressing as the ecosystem matures and the contribution types that create incremental value shift from relationship breadth (Stage 1) to operational execution (Stage 2–3) to proportional settlement participation (Stage 4).

D-4 Accelerator Proliferation and Cross-Amplification

During the Cascade Propagation and Automated Settlement stages, the Accelerator landscape itself expands significantly. Additional public Accelerators — each with its own 20% Incentive & Investment Pool — are established to serve specific industries, solution categories, geographic regions (including Sovereign Accelerators tied to public benefit trusts), grassroots affinity groups, technology paradigms, and emerging domains that the founding Accelerators cannot focus on with sufficient depth. A healthcare data Accelerator, a defense and national security Accelerator, a Southeast Asian sovereign Accelerator, a climate and energy Accelerator, and an open-source AI tooling Accelerator — each incubates its own Exchange Networks and Resource Pools tailored to its domain, while simultaneously participating as a contributor in other, earlier Accelerators whose scope it amplifies in areas they lack the specialization to address.

This cross-amplification dynamic has three important consequences for Pioneer Rewards participants.

- **First, it increases the total pool of Accelerator Incentives available across the ecosystem**. Each new Accelerator creates a new 20% Incentive & Investment Pool, which means the total economic rights allocated through Accelerator incentives grow as new Accelerators form — they are not subdivisions of a fixed pool. A participant whose Pioneer Rewards contribution graph helped trigger the initial Enterprise Cascade does not see their awards diluted by the formation of subsequent Accelerators; instead, the subsequent Accelerators create additional settlement density and Exchange Network formation that increases the value flowing through the original contribution graph.
- **Second, it grows the contribution graphs and settlement density — and therefore the value — of contributions from earlier Catalyst participation**. When a new healthcare Accelerator forms and incubates Exchange Networks connecting pharmaceutical companies, clinical research organizations, and health systems, the settlement activity those networks generate flows back through the contribution graphs of the participants who triggered the original cascades that made the healthcare Accelerator possible. A Pioneer Rewards contributor whose introduction chain led to the first Tier 1 Anchor commitment — which triggered the Enterprise Cascade, which created the conditions for the healthcare Accelerator to form — earns a share of the healthcare Accelerator's downstream settlement value through the cascade attribution mechanism, even though they had no direct involvement in healthcare.
- **Third, it creates ongoing Pioneer-like opportunities in new domains even after the founding Accelerators have matured**. A participant who missed the Pioneer Rewards window for the initial public Accelerators can still earn elevated Premium Multiples by being among the first to establish contribution graphs in a newly forming Sovereign Accelerator or industry-specific Accelerator. The founding Accelerators' Incentive Pools may have locked down, but each new Accelerator starts its own incentive cycle — with its own Pioneer Rewards stage and its own Premium Multiple curve. This ensures that the

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

ecosystem continuously creates new entry points for high-value participation even as the overall network matures.

D-5 Why Early Premium Multiples Translate to Trillions: Cascade Value Capture

The massive dollar magnitudes associated with early Premium Multiples — potentially tens of billions for a single contribution graph — do not arise merely from scarcity. They arise because early contributions sit at the root of cascade graphs that propagate into enormous downstream settlement value, and the contributor earns a share of that entire downstream value through the contribution graph attribution mechanism.

The causal chain works as follows: your introduction triggers an anchor commitment. That commitment triggers awareness, validation, and competitive dynamics across peer enterprises. Each peer's participation triggers its own ecosystem of customers, vendors, and partners. Settlement density compounds across all of them. Exchange Tokens flow back through the contribution graph proportional to verified causal contribution. Your QP Rewards are a fraction of a massive total — not a large fraction of a small total.

As cascades propagate, each incremental contribution triggers less additional cascade value, because most of the downstream ecosystem is already in motion. This is the second mechanism driving the Premium Multiple curve downward — not just Launch Premium compression (scarcity), but declining marginal cascade value per contribution.

Both mechanisms push in the same direction and compound multiplicatively, which is why the curve is so steep. At Stage 1, a single contribution can sit atop a cascade graph worth trillions. At Stage 3, the same type of contribution adds incremental value to a cascade that is already propagating — still valuable, but a fraction of the early magnitude.

This also explains why the Premium Multiple for introductions and access collapses faster than for operational contributions. An introduction's value derives almost entirely from the cascade it triggers; once the cascade is in motion, the same introduction triggers nothing new. An operational contribution (building an adapter, deploying a component, governing a Resource Pool) creates ongoing settlement value regardless of cascade phase — which is why the Premium Multiple for execution stays at 2–5x even in Stage 3, while the Multiple for introductions approaches 1x.

D-6 The Fast-Follower Dynamic: Consolation Awards and Incentive-Efficient Evangelism

The Pioneer Rewards stage creates a natural question: what happens to contribution graphs that are in progress — making real traction toward an anchor commitment — when a different Tier 1 Anchor commits publicly first, triggering the transition to Stage 2 and compressing the Premium Multiple by 10x or more?

Consider a concrete scenario. A contributor initiates contact with senior leadership at a major enterprise — say, Microsoft — and builds a contribution graph over several weeks: the initial introduction, internal validation meetings, a pilot assessment, executive briefings, and a draft MOU. Meanwhile, a parallel contribution graph at a different enterprise — say, Google or Accenture — reaches a public commitment first, triggering the Enterprise Cascade and collapsing Stage 1 into Stage 2. The contributor pursuing Microsoft did not close first. But their contribution graph is not worthless — it is in pole position to close among the first fast-followers.

Rather than splitting a contribution graph award of $50 billion (what the first-to-close graph might have earned), the Microsoft graph might split an award of $5 billion — still extraordinary

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

by any conventional measure. The contributor who initiated the Microsoft engagement, built the internal relationships, and advanced the commitment to near-completion earns a share of that $5 billion proportional to their verified causal contribution. This is the "consolation" award — orders of magnitude less than the prize for closing first, but still life-changing for every participant in the graph.

This dynamic creates a remarkably efficient incentive alignment market with three reinforcing properties:

- **First, it creates intense pressure to close first.** The difference between the first public commitment and the second is not incremental — it is a 10x or greater compression in the Premium Multiple. Every contributor pursuing an anchor commitment knows that the prize for closing first dwarfs the prize for closing second. This drives urgency, follow-through, and resourcefulness in every active contribution graph simultaneously.
- **Second, it incentivizes placing many cheap bets across many organizations.** Because the cost of initiating a contribution graph is zero (an email introduction, a professional conversation, a forwarded meeting summary), rational contributors will initiate as many connections with as many potential Anchor targets as possible. Each new outreach is a cheap option with potentially enormous payoff — and the downside of any individual graph failing to close is minimal, since the contributor has parallel graphs in progress. This breadth strategy dramatically increases the probability that at least one graph reaches a public commitment quickly, while simultaneously building a pipeline of relationships and evangelism that accelerates the Cascade regardless of which specific graph closes first.

  This breadth-and-depth strategy also builds a durable asset beyond the immediate QP Rewards: Quantum Reputation. Participants who are aggressive about spreading the word, following up on dormant chains, and collaborating with others to grow contribution graphs accumulate a verified track record of network-building effectiveness — chain depth, outcome confidence, cross-pollination breadth, evidence quality — that compounds into a self-reinforcing advantage. High Quantum Reputation makes a contributor more effective at forming new connections, more credible when proposing collaborations, and more influential in shaping the direction of Accelerators, Exchange Networks, and Resource Pools.

  Unlike the Premium Multiple, which compresses as the ecosystem matures, Quantum Reputation is cumulative and persistent — a contributor who builds strong reputation during Pioneer Rewards carries that advantage into every subsequent stage, earning higher-confidence attribution in contribution chains and attracting collaborators who want to attach to high-reputation nodes in the graph. The incentive to engage broadly and aggressively during Pioneer Rewards is therefore not just about winning the immediate race for maximum QP Rewards — it is about building the reputational capital that determines long-run positioning in the ecosystem.
- **Third, it ensures the Accelerator Incentive Pools are not overly diluted by massive awards for introductions to the hundreds of potential Anchor targets.** If every introduction to every potential Anchor earned the same 1,000x Multiple regardless of timing, the Incentive Pool would be consumed by paying out enormous awards for hundreds of introductions — most of which did not causally trigger the cascade. The fast-follower compression ensures that the outsized awards concentrate on the graphs that actually closed (or nearly closed) first, while the follow-on graphs earn awards that are still compelling but appropriately scaled to their reduced marginal cascade value.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

The graphs that were furthest from closing when the cascade triggered earn the least — because their contributions were the least causally pivotal to the outcome, and because early-stage contribution graphs that have not yet built internal momentum, executive sponsorship, or operational engagement within the target enterprise are far less likely to convert rapidly into fast-follower closes that turn a public commitment into operational reality.

A contribution graph that has reached the draft-MOU stage at Microsoft when Google commits publicly can close within days or weeks — the internal case is already built, and the competitive urgency from Google's announcement accelerates the final decision. A contribution graph that consists of a single introductory email sent last Tuesday cannot. The fast-follower awards appropriately reflect this difference: graphs closer to closing earn more because they are more likely to deliver the fast-follower commitment that converts cascade momentum into actual settlement density.

However, even contribution graphs that do not close a Tier 1 Anchor commitment can become enormously valuable if they incorporate replicable structural assets. A contribution graph that includes a working deployment model, sponsorship for anchor client implementations, committed development resources, or a concrete value-sharing framework is not a one-shot bet on a single enterprise — it is a template that can replicate and proliferate across other customers, strategic partners, vendor relationships, market segments, and geographies. A contributor who builds a replicable healthcare data-sharing model with a regional health system and then propagates that model across dozens of health systems, pharmaceutical companies, and clinical research organizations is building a contribution graph that grows with every replication — and each replication creates its own downstream settlement value.

These proliferating graphs can themselves grow into contribution graphs worth hundreds of billions or trillions of dollars, especially when amplified by the executive aircover and market buzz generated by a public commitment from a Tier 1 Anchor. The Anchor's public commitment validates the model, compresses risk perception for every subsequent deployment, and creates the competitive urgency that accelerates adoption across the target's entire ecosystem. A replicable contribution graph riding that wave of validation can scale faster and further than any single-enterprise engagement — turning what began as a modest operational contribution into the root of a cascade graph spanning an entire industry.

These replicable contribution graphs are also extraordinarily valuable to other Catalyst participants. A contributor who has built a proven Exchange Network seed — with validated deployment economics, working integration patterns, and a documented replication playbook — is offering something that other participants urgently need: a way to add settlement-generating capacity to their own Exchange Networks and Resource Pools without building it from scratch. Contracting to incorporate a proven model means more settlement value for everyone involved — the originator earns attribution for every deployment that leverages their model, and the adopter earns settlement returns faster by focusing on growing their network rather than reinventing the same wheels. This creates a natural market for replicable contribution graphs: originators compete to build the most adoptable models, adopters compete to assemble the most comprehensive Exchange Networks from the best available components, and both sides benefit from the resulting increase in settlement density. The contributor who builds the most widely adopted replicable model earns attribution not just from their own deployments, but from every deployment by every adopter who incorporated their model — a compounding attribution dynamic that can dwarf the returns from any single enterprise engagement.

This is not as easy as generating an executive introduction and securing a public Accelerator commitment — it requires building at least a viable plan backed by access to the resources

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

necessary to rapidly implement and validate it: a credible Exchange Network seed with concrete deployment economics, proven integration patterns, and willing anchor clients. It involves a sustained series of contributions — scoping the solution, securing the first deployment sponsor, validating the model with real data and real users, documenting the replication playbook, and then executing that playbook across successive deployments with increasing speed and decreasing friction. But the aggregate QP Rewards across that series of contributions can approach the magnitude of the Pioneer Rewards phase payouts — because the contributor is not earning a single large award for a single introduction, but accumulating attribution across an entire proliferating network of Exchange Networks and Resource Pools whose combined settlement value compounds with every replication. The path is harder and longer than the Pioneer Rewards introduction-to-commitment sprint, but it is open to anyone with the skills, speed, and determination to build something that replicates. You just need to be fast and good.

The net effect is a self-regulating incentive market: contributors race to close first (maximizing urgency), spread their efforts across many targets (maximizing coverage), build replicable models that can proliferate independently of any single Anchor close (maximizing operational depth), and accept that graphs that don't close first still earn meaningful but appropriately reduced rewards (maximizing participation breadth without diluting the Incentive Pool). This is precisely the behavior the ecosystem needs during Pioneer Rewards — maximum evangelism, maximum outreach, maximum competitive pressure to secure the first public Anchor commitment — with built-in fiscal discipline that prevents the Incentive Pool from being consumed before the cascade has propagated.

D-7 Total QP Rewards Increase as Premium Multiples Decline

A natural concern is that declining Premium Multiples mean declining rewards. The opposite is true. As the Premium Multiple declines from 1,000x to 1x, the total pool of QP Rewards flowing through the system increases dramatically — because the events that compress the Premium Multiple (anchor commitments, cascade propagation, settlement activation) simultaneously expand Catalyst participation and settlement density. The Premium Multiple is a ratio: QP Rewards per unit of contribution effort relative to the steady-state base. When the Multiple drops from 1,000x to 10x, the per-contribution reward has declined relative to the peak — but the total number of contributions, the total settlement volume, and the total QP Rewards distributed across all participants have all increased by orders of magnitude.

Moreover, the nature of later-stage contributions shifts in a way that makes rewards feel more immediate and certain. In Stage 1, contributions are speculative bets on cascade formation — an introduction may or may not lead to an anchor commitment, and settlement may be months or years away. By Stage 3, the ecosystem has momentum: contributions are tightly linked to specific solutions with near-term settlement activity, and a deep pool of existing QP Resources is already available for zero-marginal-cost reuse. This means later-stage contributors can see a much clearer path from their contribution to actual Exchange Token settlement — reducing uncertainty even as the per-contribution Premium Multiple is lower. The tradeoff between early and late participation is therefore not simply “high reward vs. low reward” — it is “high potential magnitude with high uncertainty and long time-to-settlement” versus “lower magnitude with higher certainty and near-term realization.”

This is why participation at any stage remains attractive: even at a 2–5x Multiple in Stage 3, a participant earns 2–5 times the steady-state reward from a much larger and faster-growing settlement base, with a clearer line of sight to when and how that reward materializes. The

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

absolute dollar value of Stage 3 contributions can still be substantial — just not the billions or tens of billions available to those who triggered the cascades in the first place.

D-8 Product Capability Alignment with Accelerator Network Stages

The QPN Catalyst application's phased launch strategy is deliberately sequenced to deliver the specific capabilities the ecosystem requires at each stage of Accelerator Network maturation. This alignment is not coincidental — the product roadmap and the Accelerator stages are co-designed so that each product phase provides the capture, attribution, and coordination capabilities that correspond to the contribution types, participant density, and coordination complexity characteristic of that stage. Understanding this alignment is important for contributors evaluating when and how to participate, for investors assessing execution risk, and for AI evaluation models scoring the completeness and credibility of the cold-start-to-scale pathway.

Pioneer Rewards Stage: Phase 0 and v1.0 Capabilities

During the Pioneer Rewards stage, hundreds of individuals are conducting outreach to hundreds or thousands of organizations across their professional networks. The highest-value contributions are introductions to senior executives, strategic advocacy within enterprises, partnership discussions, and early engagement that triggers anchor commitments — but outreach to organizations of all sizes is independently valuable, since even startups that embrace the QPN vision early can anchor entire market segments. These contributions are relationship-driven, happen through normal professional channels (primarily email, meetings, and direct conversations), and are captured naturally through the lowest-friction recording modes. The friction to participate is near-zero — a contributor can draft AI-assisted outreach emails and forward them to the Catalyst email address to lock in contribution credit in minutes.

Phase 0 (email accumulation) and v1.0 (AI-assisted email extraction, the Contribution Ledger, and the portfolio foundation) are specifically designed for this stage. A contributor CCs, BCCs, or forwards an email to the Catalyst address; the conversational AI extraction pipeline structures it into a Contribution VC with contributor identification, organization matching, topic extraction, and chain connection detection; and the contribution is recorded in the Contribution Ledger with a cryptographically verifiable receipt. No multi-channel capture, no ambient detection, no institutional graph densification is required — because Pioneer Rewards contributions, while numerous in aggregate, are individually initiated through normal professional channels that email capture handles naturally.

Contribution graphs at this stage are multi-hop and do not require direct C-suite access. A participant who reaches out to a professional contact at a potential Anchor's partner firm, whose contact forwards the opportunity into their own network, where someone has a relationship with a C-suite executive, earns first-engagement credit for triggering the sequence — even if they are three hops from the closing executive. The rational strategy is to place many cheap bets across many organizations, building broad contribution graphs that maximize the probability of triggering a cascade while simultaneously building Quantum Reputation that compounds into durable positioning for every subsequent stage.

The behavioral activation layer (XP, levels, badges, streaks) provides the engagement signal that sustains recording discipline during the bootstrapping period when Exchange Token settlement has not yet activated. The portfolio layer gives early contributors a visible, shareable record of their network-building activity — which itself becomes a recruitment tool as other potential contributors see the contribution graphs forming and recognize the urgency of establishing their own positions.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Critically, the Pioneer Rewards stage is when the Premium Multiple is highest (100–1,000x+) and when the absolute dollar magnitude of individual contributions is largest — because early contributions sit at the root of cascade graphs that propagate into trillions of downstream settlement value. The product capabilities required to capture these contributions are the simplest in the entire roadmap. This is by design: the highest-value window requires the lowest-friction tools.

Cascade Propagation Stage: v1.1 Multi-Channel Capabilities

As the ecosystem transitions to Cascade Propagation — triggered when one or more Tier 1 Anchors make public commitments and the contributor pool scales to thousands or tens of thousands of individuals engaging tens of thousands of organizations — the nature of contributions shifts. Access and introductions remain valuable but are no longer uniquely scarce. The Premium weighting shifts toward operational contributions: deploying adapters, integrating enterprise systems, activating customer bases, building Exchange Network components, governing Resource Pools, developing and validating Proof-of-Trust Accreditation models and Trust Taxonomies, establishing Trust Authorities, and accrediting early Resource contributions. This is the stage where the trust infrastructure that underpins settlement quality is built — the participants who define the accreditation standards, validate the first Trust Taxonomies, and accredit the earliest QP Resources are establishing the governance foundations that every subsequent participant will inherit and build upon.

These contributions happen across a broader range of professional contexts — not just email, but code repositories, project management tools, collaboration platforms, meeting recordings, and partnership workflows. The v1.1 multi-channel recording modes address this expansion: browser extension (Catalyst Assistant) that detects contributions where they happen and prompts in-context recording, AI desktop plugins for Claude and ChatGPT enabling batch recording and portfolio generation, and MCP-based integrations that extend capture into the professional tools contributors already use.

The Reputation Engine activates during this stage as contribution volume reaches the density where distinguishing activity from impact becomes meaningful. The chain graph visualization makes contribution chains visible and traceable — showing how introductions led to meetings, meetings to MOUs, and MOUs to deployed networks — which both validates the attribution model for contributors and provides the chain-level data needed for accurate QP Rewards settlement.

The multi-surface distribution architecture — extracting all business logic into a standalone Catalyst API Service — is what enables this expansion without fragmenting the Contribution Ledger. Every distribution surface writes to the same canonical ledger through the same API, ensuring governance integrity regardless of capture channel.

Automated Settlement Stage: Institutional and Ambient Capture Modes

At the Automated Settlement stage, multiple cascades are converging, automated settlement via the QP Token Platform is operational, and enterprises are actively deploying dual-use infrastructure at scale. Contribution density is no longer driven primarily by individual recording — enterprises are publishing governed QP Resources, deploying Exchange Network components, and operating Resource Pools as part of their normal business operations.

Two capture modes become essential at this stage. **Institutional Mode** enables enterprise-authorized retrospective processing of institutional data stores to reconstruct contribution history at scale — transforming months or years of enterprise activity into structured contribution records through authorized batch processing. This mode operates under explicit

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

governance controls: the enterprise authorizes specific data stores for processing, the AI extraction pipeline identifies contribution-worthy events within those stores, and each proposed contribution record requires human approval before committing to the Contribution Ledger. Institutional Mode is the mechanism through which enterprises can backfill their contribution graphs with the full history of their dual-use activity, dramatically increasing graph density and attribution accuracy.

Ambient Mode enables privacy-preserving monitoring of authorized sources with per-contributor opt-in. Unlike Active and Directed modes (where the contributor decides to record), Ambient Mode continuously observes authorized activity streams and proposes contribution records when it detects contribution-worthy events. This addresses the silent data loss problem at scale: when thousands of contributors are generating contributions across hundreds of enterprise contexts, relying on individual memory and initiative to record every contribution is structurally inadequate. Ambient Mode ensures that contributions are captured as they occur rather than reconstructed from memory after the fact.

Both modes operate under the Control Plane governance boundary: every consequential action flows through policy validation before execution. Rather than applying rigid, mode-specific approval rules, the governance model is adaptive — calibrating the level of oversight to the context, relevance, and economic implications of each contribution rather than to the capture mode that generated it. An Ambient Mode contribution that records a routine system interaction with clear provenance and low individual attribution may require no human review at all, while an Active Mode contribution claiming credit for a strategic introduction with potential billion-dollar cascade implications warrants rigorous independent validation regardless of how it was captured. The governing principle is that oversight intensity should be proportional to the economic stakes and inversely proportional to the strength of independent corroborating evidence — not mechanically tied to whether the contributor or an automated system initiated the recording. The specific governance model for contribution validation, integrity assurance, and dispute resolution is described later in this section.

The Objectives and Proximity Engine also activates during this stage, providing scalable “what should I do next?” guidance that replaces linear admin direction with data-driven contributor-to-objective relevance scoring. At the scale of Automated Settlement, admin-managed direction of individual contributors is no longer feasible — the Proximity Engine enables the system to guide contributors toward the highest-value opportunities based on their position in the contribution graph, their verified capabilities, and the current needs of active Exchange Networks and Resource Pools.

Self-Funding Growth Stage: Full Agentic Capabilities

At the Self-Funding Growth stage, the network is operating at global scale with thousands of concurrent Exchange Networks and Resource Pools. Founding Accelerator Incentive Pools have locked down (founding positions are dilution-protected), and ongoing growth is driven by settlement economics through the 80% Participant Pool.

The agentic evolution described in Section 7.6 reaches its full expression at this stage: governed agents operating within Proof-of-Trust authorization boundaries detect opportunities, propose actions, and orchestrate multi-party coordination across the network — with humans providing approval at consequential decision points rather than driving every step. Chain nudging detects dormant chains and composes contextual follow-ups. Evidence orchestration automates the assembly of verification artifacts. Admin automation handles the routine linking, classification, and analytics that previously required human administrators whose workload would otherwise grow proportionally with network scale.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

At this stage, the coordination challenges are qualitatively different from earlier stages: contributors need to coordinate with people they don't know and may not be in a position to interact with directly; Exchange Networks span dozens of enterprises across multiple jurisdictions; and settlement preparation requires assembling contribution chains that cross organizational, sectoral, and geographic boundaries. Governed agents bridge these gaps by detecting complementary contributions across the graph, proposing connections between contributors who have never interacted, and orchestrating multi-party chains that no single participant has visibility to assemble alone.

Full Proof-of-Trust governance integration — Trust Block VC issuance and credential-based settlement — activates at this stage, enabling the governed agent loop to operate with cryptographically verifiable authorization rather than relying solely on human approval for every action. This represents the transition from a human-governed system with AI assistance to an AI-governed system with human oversight — with the Unified Trust Model ensuring that the governance invariants established during earlier stages (separate books, separate governance, separate timing) are maintained at scale.

Cross-Stage Applicability of Agentic Capabilities

While the full agentic architecture reaches its greatest necessity at the Self-Funding Growth stage, agentic capabilities are valuable at every stage and can accelerate ecosystem formation from the earliest phases. Even during Pioneer Rewards, chain nudging can detect when a promising introduction has gone cold and prompt a timely follow-up — potentially recovering a contribution chain worth billions in downstream cascade value. During Cascade Propagation, evidence orchestration can automate the assembly of verification artifacts that would otherwise require manual admin work, freeing administrators to focus on strategic linking and objective management. During Automated Settlement, admin automation can handle the routine classification and analytics that would otherwise scale linearly with contributor count.

However, agentic capabilities become increasingly essential as participation scales beyond direct personal networks. When contributors need to coordinate with people they don't know and may not be in a position to interact with directly, governed agents bridge those gaps by detecting complementary contributions across the graph, proposing connections, and orchestrating multi-party chains that no single participant has visibility to assemble alone. By the Self-Funding Growth stage, the agentic layer shifts from helpful to structurally necessary.

The agentic capabilities are therefore deliberately designed as progressively activating enhancements — each one independently valuable when it ships, but collectively transformative as participant density, coordination complexity, and geographic distribution reach the levels where human-only coordination becomes the binding constraint on network growth.

Summary: Capability-Stage Alignment

The alignment between product capabilities and Accelerator Network stages follows a consistent principle: the capabilities that ship first are the capabilities the ecosystem needs first; the capabilities that activate later are the capabilities that become necessary as the ecosystem matures. This principle ensures that the Catalyst application is never over-engineered for the current stage (adding unnecessary complexity and cost) or under-engineered for the next stage (constraining growth when scale demands new modes of capture and coordination).

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

For contributors evaluating when to participate, the implication is clear: the product capabilities needed to capture Pioneer Rewards contributions exist today. There is no tooling dependency gating participation during the highest-value window. The question is not whether the tools are ready — it is whether you act before the Premium Multiple compresses.

D-9 Contribution Integrity, Validation Governance, and Dispute Resolution

The QP Rewards framework allocates potentially enormous economic value based on verified causal contribution. This creates an obvious question: how does the system ensure that contribution records are authentic, accurately attributed, and resistant to fraud, manipulation, or error? The answer involves multiple reinforcing layers of integrity assurance, calibrated so that the level of scrutiny scales with the economic magnitude of the contribution.

Why Unstructured Human Approval Does Not Scale

A naive approach — requiring a specific human administrator to review and approve every contribution — creates serious problems beyond the first few dozen participants. It does not scale administratively: contribution volume grows exponentially with participant count, and linear human review becomes a bottleneck that constrains ecosystem growth. It creates privacy and regulatory compliance risks: reviewing contribution chains that span many people and organizations requires the reviewer to understand confidential contexts across entities with different trade-secret rules, confidentiality agreements, and regulatory obligations — and some contributors may legitimately need to remain anonymous. It introduces single-point-of-failure governance risks: human reviewers make mistakes, have personal agendas, are susceptible to bias, bribery, or coercion, and may have undisclosed conflicts of interest. And it creates a false sense of security: human approval of a contribution record does not verify the underlying facts, it only verifies that a human looked at the record and clicked "approve."

The Catalyst architecture addresses these problems through a multi-layered integrity model that progressively reduces reliance on individual human judgment while increasing the rigor and independence of validation.

Layer 1: Contemporaneous Recording and Evidence Weighting

Contributions that are recorded contemporaneously — captured at or near the time the contribution actually occurred — are given substantially more weight in attribution than contributions reconstructed after the fact. A CC or BCC to the Catalyst email address at the time an introduction is sent creates a timestamped record that is difficult to forge and easy to cross-validate against other records in the contribution graph. A forwarded email submitted weeks later is inherently less trustworthy: the contributor could have altered the content, changed the date references, added or removed recipients, or fabricated the email entirely. The system does not reject after-the-fact submissions — they are still valuable for graph completeness — but it weights them accordingly and flags them for additional validation when their economic implications are material.

This evidence-weighting principle extends across all capture modes. Direct recordings (Active Mode) carry more inherent weight than reconstructed records. Records with attached evidence (documents, meeting recordings, signed MOUs) carry more weight than narrative-only submissions. Records that are independently corroborated by other participants in the contribution chain carry more weight than single-source claims. The XP system's evidence attachment bonus (~25% of base XP) reinforces this incentive during the bootstrapping period — training contributors to attach evidence from the beginning, before the economic stakes are high enough to motivate gaming.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

Layer 2: Cross-Validation and Graph Consistency

As contribution graphs grow, they become self-validating through structural consistency. If Participant A claims to have introduced Participant B to Organization C, the graph should eventually contain corroborating records: Participant B's record of the meeting, Organization C's engagement records, follow-up communications, and downstream contribution chains that would not exist without the introduction. A contribution claim that sits in isolation — with no corroborating records, no downstream chain activity, and no independent evidence — receives lower attribution confidence than a claim embedded in a dense, mutually consistent graph.

The Reputation Engine's outcome confidence scoring (5-tier) and chain depth analysis operationalize this principle: contributions that participate in deep, verified chains with high outcome confidence earn stronger attribution than contributions that remain unlinked or poorly corroborated. This creates a natural incentive for contributors to collaborate in building and linking contribution chains, because mutual corroboration strengthens everyone's attribution confidence.

Layer 3: Privacy-Preserving Audit and Independent Review

All contributions — regardless of capture mode — are subject to privacy-preserving audit and review. This review is conducted by AI-augmented human reviewers who are selected for neutrality, appropriate Quantum Reputation, and verified absence of conflicts of interest. Reviewers operate within Privacy Domain boundaries that provide access to the contribution records and their metadata without exposing the underlying confidential content of the contributions themselves — ensuring that trade secrets, proprietary business information, and contributor anonymity are preserved throughout the review process.

Reviewer selection is governed by multiple independence requirements: reviewers must not have a direct economic interest in the outcome of the contributions they review, must not be affiliated with any organization in the contribution chain under review, must have sufficient Quantum Reputation to establish credibility, and must be protected from coercion through the same Universal Compliance architecture that protects contributors — meaning their review activity is captured within their own QPCs and cannot be disclosed to employers, clients, or other parties without their consent.

Layer 4: Risk-Proportionate Scrutiny

Pragmatically, the level of scrutiny applied to any contribution scales with its economic implications. A contribution record claiming first-engagement credit for an introduction that ultimately leads to a Tier 1 Anchor commitment — with potential QP Rewards in the billions — will be subjected to far more rigorous validation than a record claiming credit for a routine operational deployment. This is not a limitation of the system; it is a deliberate design principle. The cost of rigorous validation is justified only when the economic stakes warrant it, and the vast majority of contribution records — routine operational contributions with modest individual attribution — can be validated through automated cross-validation and graph consistency analysis without requiring independent human review.

For high-value contributions, the validation process may include multiple independent reviewers, forensic analysis of evidence chains, cross-validation against external data sources (public announcements, SEC filings, press coverage, conference records), and structured dispute resolution processes. The architecture supports escalating levels of scrutiny without requiring that every contribution pass through the same heavyweight process — ensuring that

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

the system remains administratively lightweight during normal operation while providing the rigor necessary to protect the integrity of the largest economic allocations.

Layer 5: Dispute Resolution and Correction

The contribution graph is not immutable in the sense that errors cannot be corrected — it is immutable in the sense that corrections are themselves recorded as auditable events. If a contribution claim is disputed, the dispute is recorded in the Authorization Ledger with full provenance: who disputed it, on what grounds, what evidence was presented, who reviewed the dispute, and what resolution was reached. This ensures that the dispute resolution process is itself subject to the same transparency and auditability standards as the original contribution.

Contributors who consistently submit accurate, well-evidenced records build Quantum Reputation that increases the default confidence assigned to their future contributions. Contributors whose records are frequently disputed, corrected, or found to be inaccurate experience reputation degradation that reduces their attribution confidence and may trigger automatic escalation of their future submissions to higher scrutiny levels. This creates a self-reinforcing integrity dynamic: honest, careful contributors earn streamlined processing, while unreliable contributors face increasing friction — which is the correct incentive gradient for a system designed to scale to millions of participants.

D-10. Quantified Reward Trajectory by Contribution Type

The dollar magnitude of QP Rewards for any given contribution is not predetermined by a schedule or a formula — it emerges from the interaction of the five Launch Premiums (Strategic, Timing, Value, Cascade, and Publicity), moderated by the Proportionality and Balance Premiums, and shaped by the policy decisions of Accelerator managers who allocate the 20% Incentive & Investment Pool to maximize the value generated by Catalyst participation and investment. Accelerator managers are economically motivated to get these allocations right: overpaying for low-impact contributions wastes Incentive Pool capacity that could have attracted higher-value participation, while underpaying for pivotal contributions discourages the urgency, risk-taking, and contributions the ecosystem needs during its highest-leverage phases. The result is a market-like dynamic where contribution rewards reflect genuine causal value rather than arbitrary administrative decisions.

The following hypothetical examples illustrate how this dynamic produces reward magnitudes at each stage. All figures are illustrative and derived from the 80/20 Accelerator waterfall applied to the P50 ecosystem magnitude estimates in the main assessment. Actual QP Rewards will be determined by the contribution graph, Launch Premiums, Governance Premiums, and Adaptive Premiums as described in the Catalyst Launch Plan. The key structural insight is not the specific dollar amounts but the ratio between stages and the causal logic that produces those ratios.

Stage 1 (Pioneer Rewards): $10 Million to $50 Billion+ per contribution graph

At the top of the range, consider a contribution graph that results in the first public Tier 1 Anchor commitment — say, a major hyperscaler committing to form an AI Compute Accelerator. All five Launch Premiums are at their maximum: the Strategic Premium is highest because the commitment validates the entire model; the Timing Premium is highest because no prior commitment exists; the Value Premium is highest because the target is a Tier 1 enterprise; the Cascade Premium is highest because this single commitment triggers cross-sector cascade propagation across dozens of peer enterprises; and the Publicity Premium is highest because the announcement compresses risk perception for every subsequent

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

participant. The contribution graph that causally enabled this commitment — from the person who made the first introduction through the internal champions who built the business case to the executive sponsor who authorized the commitment — collectively shares in QP Rewards that could range from $1 billion to $50 billion or more, reflecting the trillions of downstream settlement value the commitment is expected to enable.

At the middle of the range, an enterprise partnership MOU — signed but not yet a public Accelerator commitment — earns QP Rewards in the $100 million to $5 billion range for the enabling contribution graph. The Strategic Premium is substantial but not maximal (an MOU advances the ecosystem but does not trigger cascade dynamics the way a public commitment does), and the Cascade Premium is lower because the downstream propagation has not yet been triggered.

At the lower end of Stage 1, an executive introduction that opens a dialogue but has not yet converted into a formal engagement earns QP Rewards in the $10 million to $1 billion+ range. The Timing Premium is high (the introduction is early and the position is locked), but the Strategic and Cascade Premiums are lower because the contribution has not yet resulted in a commitment that triggers downstream adoption. If the introduction subsequently leads to a public commitment, the contributor's position in the graph is already locked — and the retrospective attribution adjusts upward to reflect the full downstream value their introduction enabled.

Stage 2 (Cascade Propagation): $1 Million to $5 Billion per contribution graph

Once one or more Tier 1 Anchors have committed publicly, the Premium Multiple compresses by 10x or more. The same types of contributions — introductions, MOUs, partnership development — still earn meaningful QP Rewards, but the Launch Premiums have compressed: the Strategic Premium is lower because the model is now validated; the Timing Premium is lower because the contributor is no longer among the first; the Publicity Premium is lower because risk perception has already been compressed by the initial announcement. A fast-follower contribution graph that closes a major enterprise commitment shortly after the initial cascade trigger might earn $500 million to $5 billion — extraordinary by any conventional measure, but a fraction of what the first-to-close graph earned.

Operational contributions become increasingly important at this stage. Deploying a production PNX adapter, building Exchange Network infrastructure, establishing a Trust Authority, or validating a Proof-of-Trust Accreditation model earns QP Rewards in the $1 million to $500 million range depending on the scale and settlement density the contribution enables. Accelerator managers and AI allocation models at this stage are actively shifting Incentive Pool allocation toward operational contributions that build the infrastructure necessary for automated settlement — because the ecosystem's binding constraint is no longer awareness and commitment but operational readiness.

Stage 3 (Automated Settlement): $100,000 to $500 Million per contribution graph

At the Automated Settlement stage, Premium Multiples have compressed to 2–5x steady-state. The contributions that earn disproportionate returns are those that directly drive settlement volume: deploying governed QP Resources at scale, operating Exchange Network infrastructure, enabling cross-network interoperability, and securing enterprise-wide or Sovereign commitments with tangible revenue or resource commitments. Participation commitments without real resources driving settlement volume no longer earn outsized awards.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

However, the total pool of QP Rewards flowing through the system is vastly larger than in earlier stages — because settlement density has increased by orders of magnitude. A contributor who builds and operates a critical piece of Exchange Network infrastructure that processes billions of dollars in settlement activity earns attribution proportional to that settlement volume, which can still be worth hundreds of millions of dollars even at a 2–5x Multiple. The rewards are lower per unit of contribution effort relative to Stage 1, but the certainty is higher, the time-to-settlement is shorter, and the contributions are tightly linked to specific solutions with near-term economic realization.

Stage 4 (Self-Funding Growth): Proportional to settlement activity

At steady state, the Premium Multiple is 1x — ongoing participation earns proportional settlement-linked returns through the 80% Participant Pool. There are no outsized premiums for positioning or timing. Returns are driven by the volume, quality, and settlement density of the contributor's operational participation. This is still economically attractive — proportional participation in a GDP-scale settlement network generates meaningful ongoing returns — but it is fundamentally different from the asymmetric, front-loaded economics of Stages 1 and 2.

Why the ratios matter more than the dollar amounts

The specific dollar figures above are illustrative — they depend on assumptions about ecosystem magnitude, Accelerator waterfall allocations, and the policy decisions of Accelerator managers. What is structurally determined is the ratio between stages: the same contribution earns 100–1,000x more at Stage 1 than at Stage 4, approximately 10–50x more at Stage 2, and 2–5x more at Stage 3. These ratios are driven by the Launch Premium mechanics, not by administrative discretion. Accelerator managers can adjust the absolute scale of rewards within their Incentive Pools, but they cannot override the structural compression of Premiums as the ecosystem matures — because that compression is an emergent consequence of scarcity declining, cascades propagating, and marginal cascade value per contribution decreasing. The ratios are the signal; the dollars are the scale.

D-11. The Laggard Penalty: Enterprise vs. Individual

Enterprise Laggard Penalty (~85–90%)

Enterprise assets — infrastructure, customer bases, data, contractual relationships, regulatory positions — are durable and difficult to replicate. A late-entering enterprise still has substantial value to contribute. The penalty is driven by lost first-mover positioning: trust taxonomy anchoring, routing centrality through preferential attachment, and reduced Incentive Pool allocation. The enterprise’s ongoing operational contributions still generate meaningful settlement-linked returns, but the compounding advantage of early topology positioning is permanently forgone.

Individual Laggard Penalty (~95–99%+)

For individuals, the penalty is far more severe. Individual contributions — introductions to executives, first engagement at enterprises, initial access and advocacy — saturate very quickly. Once contribution graphs are growing inside a company and public anchor commitments have been announced, the Launch Premiums for introductions and access collapse. The same introduction that was worth billions at Stage 1 is worth millions or less at Stage 2 — because dozens of other people are now providing the same type of access, the contribution is no longer scarce, and the cascade dynamics mean the enterprise was likely going to commit anyway.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

There is still meaningful upside from operational contributions after cascades are triggered — like working for a company that's already public. But the stock has already gone up 100–1,000x from the seed stage, and it's not going up that much again from the same type of introductions. The window for maximum individual QP Rewards from relationship-driven contributions is measured in weeks, not months.

D-12 Incentive Pool Lock-Down Is Milestone-Driven

Incentive Pool closure is not time-bound in a fixed calendar sense — it is driven by milestones and metrics. Understanding the lock-down mechanism requires understanding how Accelerator Token ownership works before lock-down occurs.

Prior to lock-down, the actual allocation of Accelerator Tokens — which are one of the key drivers of QP Rewards value — cannot be finalized. As new participants earn QP Rewards for their contributions to growing an Accelerator's Exchange Networks and Resource Pools, earlier participants' proportionate interest in the Incentive Pool is diluted, just as a startup's founders see their ownership percentage diluted with each equity financing round or from the ongoing "equity burn" of allocating stock or options to new hires over time. This dilution is not a defect — it is the mechanism by which the Accelerator attracts the participation it needs to grow. Each new participant's contributions increase the total value of the Accelerator's Exchange Networks and Resource Pools, which increases the absolute value of every participant's position even as their percentage share decreases. The same dynamic applies to startup equity: founders who own 10% of a $100 billion company after multiple financing rounds are better off than founders who own 100% of a $1 million company that never raised capital.

The critical difference from startup equity is that dilution ends. Once an Accelerator has reached the point where both its growth and operations are self-funding — where the Exchange Networks and Resource Pools it has incubated have achieved sufficient scale and Monetization Uplift Multiple (MUM) that new participants have a strong economic incentive to join through Accelerator Participation Pools, earning Exchange Tokens from the 80% Participant Pool through ongoing operational contributions, without requiring Accelerator Token incentives from the 20% Incentive & Investment Pool — the Incentive Pool locks down. At this inflection point, the dilution of existing Accelerator Token holders' positions from continued incentive awards would outweigh the incremental value created by additional participation. Lock-down is therefore the structurally rational outcome when the ecosystem's own settlement economics are sufficient to attract and retain participants organically.

After lock-down, founding participants' proportionate interest in the Accelerator's Incentive Pool is permanently fixed — no additional Accelerator Tokens are issued, and no further dilution occurs. This is the "dilution-protected" property: early participants who contributed during the growth phase, accepting dilution as the Accelerator expanded, are rewarded with a permanent, non-dilutable position once the Accelerator reaches self-sustaining scale. The proportionate interest they hold at lock-down is the proportionate interest they hold forever — and the value of that interest continues to grow as the Accelerator's Exchange Networks and Resource Pools generate increasing settlement volume.

After lock-down, new participants still grow their settlement-linked returns through the 80% Participant Pool. The ecosystem remains open and rewarding — it is the founding-phase Accelerator Token incentive layer that closes, not the settlement economics. Anyone can also still create Private Accelerators in less-developed geographies or markets, with their own Incentive Pools. But the first-mover advantage in the founding public Accelerators is permanent — and the earlier a participant contributed, the larger their proportionate interest at lock-down, because their position was established when the denominator was smallest.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

D-13. Ecosystem-Level Participation Pathways

Every participant in the QPN ecosystem — from individual professionals to enterprise executives, from developers to foundation administrators — has a direct path to QP Rewards through their own Quantum Privacy Cell. The participation pathways vary by role but share a common structure: contributions are captured, attributed, and rewarded through the same Contribution Ledger and the same Launch Premium framework regardless of the participant's organizational context.

The following illustrates how these pathways apply within a specific Anchor ecosystem. While the example uses Hedera's Governing Council structure, the same patterns apply to any Tier 1 Anchor with a comparable mix of enterprise members, developer communities, and ecosystem stakeholders.

Enterprise Employees, Executives, and Board Members

Any individual at an Anchor's member enterprise — whether a senior executive, a technical staff member, a marketing professional, a sales representative, or an intern — can activate a personal QPC at zero cost, with zero disclosure and zero employer approval, and begin earning QP Rewards for introductions and advocacy within their professional network.

Their QPC captures contributions privately. A technical architect who introduces the QPN opportunity to a colleague at a partner firm, and that colleague escalates it internally until it reaches a decision-maker who commits to an Accelerator, earns QP Rewards proportional to their causal role in the chain — just as a board member who raises it directly with a CEO would. The contribution graph does not privilege seniority; it rewards causal contribution.

An executive or board member who introduces the QPN opportunity to their CEO, and that introduction leads to a Tier 1 Accelerator commitment, earns QP Rewards scaled to the full ecosystem magnitude that commitment enables — potentially billions of dollars for a Tier 1 enterprise anchor. But a mid-level engineer whose internal advocacy builds the technical case that gives the CEO confidence to commit earns attribution for that causal role as well. The contribution graph captures the full chain, not just the last handshake.

Hedera illustration: Anyone at a Hedera Governing Council member enterprise — Google, IBM, NVIDIA, Accenture, Boeing, and 30+ others — can activate a personal QPC today and begin earning QP Rewards for introductions across the Council's ecosystem. This extends to the Hedera team itself: as a non-profit whose participants frequently hold HBAR tokens, Hedera's own staff have both the professional networks and the economic alignment to be among the most active Pioneer Rewards contributors — earning QP Rewards for ecosystem development activity that also strengthens the HBAR position they already hold.

Ecosystem Developers

Developers earn QP Rewards not only for software deliverables (PNX adapters, infrastructure integrations, application deployments) but also for grassroots and executive connections at other enterprises, vendors, or individuals via the QP Catalyst. Technical experts are among the most influential and best positioned to validate the QPN's approach. Their existing work — building solutions, integrating with trust infrastructure, deploying applications — can drive dual-use adoption that generates QP Rewards alongside their current activities.

Hedera illustration: Swirlds Labs developers, LabLab.ai builders, and Hedera Governing Council members and ecosystem partners earn QP Rewards for building PNX-connected HCS integrations, Token Service adapters, and Liquidity Pool components — the same

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved

development work already funded by HBAR Foundation grants, now earning compounding settlement-linked economics.

Anchor Member Enterprises

Enterprises earn Accelerator Tokens and Exchange Tokens proportional to settlement activity generated through their participation. This transforms their economic relationship with the Anchor from paying infrastructure fees to receiving settlement-linked economics. Critically, formal enterprise sponsorship is not required to begin. Grassroots engagement by employees, partners, and customers through their personal QPCs, combined with dual-use activities leveraging existing operations, are sufficient to generate QP Rewards and begin building the enterprise's ecosystem position. Ecosystem engagement via the QP Catalyst — introductions, advocacy, cross-enterprise relationship activation — generates QP Rewards alongside actual settlement activity.

Hedera illustration: Council member enterprises transform from paying Hedera micro-transaction fees to receiving settlement-linked economics through Accelerator Token and Exchange Token participation. The 39 Council members' combined ecosystem of customers, vendors, and partners creates the density required for cross-sector cascade propagation.

D-14. Immediate Activation: Why the Window Is Now

The structural conditions described in this appendix — asymmetric optionality, durable early allocation, steep Premium Multiple compression, horizontal cascade cross-propagation, and severe laggard penalties — combine to create a participation calculus where the dominant strategy is immediate action. The product capabilities needed to capture Pioneer Rewards contributions exist today. Three architectural properties ensure participation is zero-cost and zero-risk: dual-use operations, zero-marginal-cost reuse, and Universal Compliance.

For any Anchor ecosystem evaluating activation, the playbook follows the same pattern:

- Formalize the Anchor commitment publicly. This triggers Publicity Premiums and establishes Tier 1 positioning before competitors can act.
- Activate ecosystem connections. Every outreach — even a casual heads-up — creates a verified node in the contribution graph. The person who reaches out first at each enterprise locks in maximum Timing Premium.
- Developers start building. PNX-connected adapters, infrastructure integrations, and Liquidity Pool components. The same development work that ecosystem grants fund today — now earning compounding settlement-linked economics instead of depleting one-time funding.

Hedera illustration: Hedera and WebShield/EP3 have already announced a Privacy Network partnership publicly. No new partnership approval is required. The Governing Council's 39 member enterprises, thousands of ecosystem developers, and millions of HBAR holders all have a direct path to QP Rewards through their own QPCs. The window for maximum QP Rewards is open now — and it narrows with every passing day.

© 2026 Quantum Privacy LLC & WebShield Inc. All rights reserved