PROVISIONAL PATENT APPLICATION

Systems & Methods for a Self-Funding, Self-Organizing Quantum Privacy Exchange and Accelerator Network

Provisional Filing Date: December 4th, 2025 **Application #**: 63/931,387

Inventors: Jonathan Paul Hare (CEO), Richard Arthur Muth (CTO)

Applicant/Assignee: WebShield, Inc. (Delaware)

ABSTRACT

The invention provides systems and methods for automated, privacy-preserving governance, compliant digital participation, and trust-verified value exchange across distributed, multi-jurisdictional ecosystems. At its core, the architecture enables the confidential creation, dormant maintenance, and continuous compliance verification of **Quantum Privacy Cells (QPCs)**—limited-liability governance compartments that function as the lawful participation boundary for individuals, enterprises, institutions, and governmental entities. Each QPC is paired with a **Personal** or **Enterprise Privacy Network (PPN/EPN)** that serves as the participant's operational agent, enabling privacy-preserving identity, consent, rights assertion, delegated authority & cross-organizational workflows.

A unified governance substrate—comprising a **Unified Trust Model (UTM), Proof-of-Trust (PoT)** verification, and interoperable **Trust Taxonomies**—transforms legal, regulatory, fiduciary, and ethical obligations into executable policy logic. Rights, capabilities, and tokenized interests remain inactive until all eligibility criteria are satisfied; non-eligible or conflicted rights are automatically reclassified and redirected to compliant substitutes or **Public-Benefit Derivative Rights (PBDR)** pools with full cryptographic provenance.

The invention further establishes a global, privacy-preserving universal exchange fabric via an AI-powered **Quantum Privacy Exchange (QPX)** and **Quantum Privacy Accelerators (QPAs)**. Any lawful resource—data, models, content, algorithms, workflows, permissions, human services, devices, infrastructure, financial or ecological assets, contractual or regulatory rights, business processes, governance assets, trusted relationships, engagement, expertise, or institutional capabilities—**may be tokenized, orchestrated, virtually pooled, reprocessed, and repeatedly reused at zero marginal cost**. This enables the creation of composite or derivative resources without duplicating data, computation, or agreements, while enforcing the Trust Criteria governing the full lineage of all contributing inputs and allocating value accordingly. These capabilities allow **personalized AI and efficient, trust-verified markets to operate across the economy, unlocking dramatic productivity gains while ensuring end-to-end compliance** with all privacy, cybersecurity, legal, regulatory, and contractual requirements. The result is a privacy-preserving, freely available global marketplace that benefits all of society.

Critically, the architecture achieves these capabilities through **dual-use deployment**. QPCs, PPNs, and EPNs expose resources through the rights, APIs, workflows, devices, identity systems, infrastructure, and spending streams that organizations and individuals already use, in ways that can't be detected or blocked. This enables the network to operate freely on top of existing business practices—without requiring system replacements, data consolidation, central integration, or vendor cooperation—and makes the resulting exchange fabric freely available and difficult to block, detect, or prohibit. This vastly **reduces the capital investment, incumbent vendor buy-in, and governmental approvals** typically required to launch and globally scale societal-scale infrastructure.

Verified contributions, lawful participation, and resource reuse generate measurable value recorded as encrypted Trust Blocks, enabling **incentive-aligned collaboration without exposing personal identities, proprietary information, or regulated data**.

A key aspect of the invention is its ability to **self-fund and bootstrap its own development and global adoption**. Individuals, enterprises, institutions, public agencies, and investors may contribute resources they already control—data, models, workflows, permissions, governance assets, devices, infrastructure, relationships, and expertise—using their existing contractual rights. These contributions are recorded as confidential, cryptographically verifiable lineage within QPCs and **automatically recognized through Resource Tokens, Exchange Tokens, or other Quantum Privacy Tokens or derivative-rights structures, all without forming inducements, securities interests, or cross-organizational conflicts of interest**. Because contributions require no centralized approval, procurement, or integration, the architecture enables **zero-marginal-cost crowdsourcing** of its own development and proliferation. Each early contribution—introductions, onboarding new enterprises, compliance validation, governance design, revenue-sharing agreements, dual-use infrastructure, etc. —creates durable tokenized value that accelerates further adoption and network growth. This dynamic **allows the platform to scale organically using billions of existing devices, APIs, workflows, and legal agreements long before full QPX deployment**.

A **Quantum Rating System (QRS)** derives trust, compliance, contribution, quality, safety, network leverage, and public-benefit metrics directly from the **global Privacy Graph**, evaluating the full cryptographically verified lineage and provenance of any asset, participant, process, or computational output **without exposing underlying records or compromising privacy**. Because all lineage elements are represented as encrypted Trust Blocks, the QRS can simultaneously compute diverse rating schemes in Quantum Privacy Domains in parallel—legal, ethical, fiduciary, clinical, environmental, financial, operational, or sector-specific—each drawing from the same privacy-preserving data structures. These metrics may be independently weighted, recombined, or interpreted to

generate **hundreds or thousands of concurrent rating schemes with extreme computational efficiency and low latency**, enabling real-time market formation, solution orchestration, and cross-domain optimization. This makes it possible to **simultaneously satisfy and optimize against the disparate goals, incentives, and Trust Criteria of billions of participating individuals, enterprises, systems, and devices,** all while maintaining strict privacy, security, and regulatory compliance.

Financial and liquidity mechanisms—including **Quantum Privacy Liquidity Pools**, trust-verified settlement structures, tokenized entitlements, and privacy-preserving proofs of verified income or asset value—enable liquidity provisioning, securitization, cross-jurisdictional settlement & automated tax treatment without compromising confidentiality.

The invention also provides a **Privacy-Preserving Process Optimization Service (PPOS)** that uses distributed computation and PoT-verified orchestration to improve efficiency, compliance, sustainability, and equitable value allocation across personal, enterprise, governmental, and societal workflows.

Together, these mechanisms create a unified, trust-verified digital infrastructure in which privacy, compliance, reuse, and governance are intrinsic architectural properties. The invention enables lawful, transparent, universal, and self-funding collaboration at global scale—**unlocking continuous innovation, equitable participation, zero-marginal-cost resource reuse, and measurable societal benefit across all sectors of the economy**.

TABLE OF CONTENTS

CROSS-REFERENCE TO RELATED APPLICATIONS

This application **relates to** U.S. Patent Application No. **19/206,859**, filed **May 13, 2025**, titled *"Quantum Privacy, Proof of Trust, and Privacy Network Exchange,"* which itself is a **Continuation-in-Part** of U.S. Patent No. **12,316,610 B1**, titled *"Privacy Network and Unified Trust Model."*

This application further **claims the benefit of priority under 35 U.S.C. § 119(e)** to the following U.S. **Provisional Patent Applications**, each incorporated by reference in its entirety:

- U.S. Provisional Patent Application No. **63/804,583**, filed **May 12, 2025**, titled *"Quantum Privacy, Proof of Trust, and Privacy Network Exchange";*
- U.S. Provisional Patent Application No. **63/895,861,** filed **October 7, 2025**, titled *"Systems and Methods for Trust-Verified Tokenization & Settlement";* and
- U.S. Provisional Patent Application No. **63/923,253**, filed **November 22, 2025**, titled "*Systems and Methods for Quantum Privacy-Enabled Self-Funding AI Trust, Safety & Compliance"*

- U.S. Provisional Patent Application No. **63/926,629**, filed **November 27, 2025**, titled *"Systems and Methods for Quantum Privacy-Enabled Personalized, Value-Based Universal Exchange for Better Health"*

All of the foregoing applications are **commonly assigned to WebShield, Inc. (Delaware)** and are **incorporated by reference** for purposes of **priority and enablement**.

Field of the Invention

The present invention relates to systems and methods for establishing, governing, and optimizing lawful digital participation, privacy-preserving computation, compliant resource pooling, and trust-verified economic coordination across individuals, enterprises, institutions, and governmental entities. More specifically, the invention concerns the confidential creation, management, activation, and continuous compliance verification of limited-liability governance compartments—referred to herein as **Quantum Privacy Cells (QPCs)** or functionally equivalent legal constructs—that enable individuals or organizations to participate in distributed ecosystems under conditions of **deferred activation**, **auditable provenance**, and **machine-enforced legal and ethical compliance**.

The invention further relates to the operation of **Personal Privacy Networks (PPNs)** and **Enterprise Privacy Networks (EPNs)** that serve as privacy-preserving agentic environments for identity, consent, rights assertion, contractual execution, cross-organizational workflows, and delegated authority structures.

These Privacy Networks interoperate through a universal governance substrate defined by a **Unified Trust Model (UTM)**, **Proof-of-Trust (PoT)** verification, and **Trust Taxonomies** that map legal, regulatory, ethical, and contractual constraints into machine-executable policy logic.

The invention additionally concerns automated systems for enabling **zero-marginal-cost formation**, **lifecycle management**, and **reconstitution** of large populations of Quantum Privacy Cells; for enforcing fiduciary, employment, ethics, and jurisdiction-specific prerequisites prior to any activation of rights or value; and for rerouting restricted or unvestable interests into **Public-Benefit Derivative Rights (PBDR)** pools or compliant substitutes with full cryptographic provenance.

Beyond governance, the invention relates to **trust-verified market formation** through **Quantum Privacy Accelerators (QPAs)** and the **Quantum Privacy Exchange (QPX)**, which together enable lawful, privacy-preserving pooling of human, digital, financial, and ecological resources. These systems establish **self-funding, continuously liquid market structures** governed by verifiable trust signals, domain-specific Trust Criteria, and incentive-aligned participation models. They further support cross-organizational and

cross-jurisdictional collaboration without requiring disclosure of personal identity, proprietary information, or regulated data.

The invention also encompasses the automated operation of **Quantum Rating Systems**, including trust, compliance, safety, contribution, network-leverage, value-amplification, and public-benefit metrics. These ratings are derived from **encrypted lineage and provenance** stored within the global Privacy Graph and may be computed using privacy-preserving cryptographic techniques to support routing, valuation, contractual terms, liquidity provisioning, incentive alignment, public-benefit allocation, and systemic optimization.

In addition, the invention includes privacy-preserving financial, fiscal, and liquidity mechanisms—such as **Quantum Privacy Liquidity Pools (QPLPs)**, **tokenized resource and solution-exchange mechanisms**, **restricted and derivative rights structures**, and **compliance-verified securitization frameworks**—that allow lawful financial participation, cross-jurisdictional settlement, automated tax treatment, and efficient capital formation while maintaining strict privacy, regulatory conformity, and provenance integrity.

Finally, the invention encompasses a **Privacy-Preserving Process Optimization Service (PPOS)** and related agentic optimization frameworks that analyze, negotiate, and improve workflows, contracts, and resource allocations using privacy-preserving computation. Acting across commercial, governmental, institutional, civic, and personal domains, the PPOS enables a lawful, auditable, continuously improving global market for efficiency, sustainability, safety, and value creation.

Collectively, these mechanisms create an integrated, trust-verified digital infrastructure that unifies legal governance, privacy-preserving computation, compliant collaboration, equitable value exchange, and incentive-aligned optimization. The invention transforms privacy, regulation, compliance, and governance from external constraints into **intrinsic system-level properties**, enabling lawful, transparent, and self-funding global coordination among individuals, enterprises, and governments—while preserving confidentiality, ethical integrity, security, and regulatory accountability at every step.

1. Overview of the Invention

The present invention provides a unified legal, computational, and economic infrastructure for lawful, privacy-preserving digital participation, decentralized collaboration, and continuous market formation at population scale. It integrates four foundational components—**Quantum Privacy Cells (QPCs)**, **Personal and Enterprise Privacy Networks (PPNs/EPNs)**, the **Unified Trust Model (UTM)** with **Proof-of-Trust (PoT)** verification, and the **Quantum Privacy Exchange (QPX)**—into a single, coherent

framework that enables individuals, enterprises, institutions, and governments to coordinate, transact, share, and repeatedly reuse resources at effectively zero marginal cost, while satisfying all confidentiality, fiduciary, ethical, regulatory, and data-protection obligations across jurisdictions.

At its core, the invention replaces today's fragmented, compliance-constrained economy and institutional landscape—in which enterprises, governments, communities, and digital systems operate within isolated legal and operational silos—with a **unified, privacy-native, trust-verified governance fabric**. Rather than constraining coordination to the digital layer, the invention addresses the deeper structural fragmentation that has historically prevented lawful, cross-sector collaboration across regulatory regimes, contractual boundaries, infrastructures, and organizational constraints.

Every participant—whether an individual, enterprise, institutional investor, public agency, autonomous system, or cross-sector consortium—interacts through a **Quantum Privacy Cell (QPC)**: a confidential, limited-liability governance compartment that remains dormant and undiscoverable until eligibility, consent, authority, and compliance requirements are cryptographically verified. QPCs serve as the atomic units of lawful identity, rights management, delegation, accountability, and participation across the socio-economic system. They allow statutory rights to be asserted, fiduciary duties to be honored, inter-institutional agreements to be executed, and resources or services to be contributed without revealing personal, institutional, or proprietary information.

Through these mechanisms, the invention establishes a **universal, zero-marginal-cost exchange fabric**. Any lawful resource—including but not limited to **data and data rights** (personal, proprietary, biomedical, IoT, industrial), **digital assets** (content, software, algorithms, AI models or agents), **computational or physical infrastructure**, **human-centric services, expertise, and professional labor**; **engagement and trusted relationships**; **brands and forms of influence**; **legal, contractual, regulatory, and IP-based rights**; **governance assets**; **nature-based resources** (land, water, biodiversity, carbon or ecological credits); **financial instruments**; **real assets**; and **knowledge-based assets**—can be tokenized, orchestrated, recombined, syndicated, and reused across sectors without duplicating data, renegotiating agreements, or rebuilding integrations.

The **Unified Trust Model (UTM)** and **Proof-of-Trust (PoT)** architecture transform legal, fiduciary, contractual, and regulatory obligations into **machine-enforceable logic**. Each operation—data access, contractual execution, delegation, resource contribution, model invocation, optimization, token issuance, value attribution, or policy enforcement—occurs only when **cryptographically verifiable Trust Credentials** satisfy the Trust Criteria of the relevant stakeholders. When conditions are not met, the system automatically suspends, adapts, or reclassifies rights; substitutes compliant actors or workflows; or redirects

restricted value to **Public-Benefit Derivative Rights (PBDR)** pools, thereby maintaining lawful continuity without exposing identities, internal processes, or proprietary rule systems. This creates the first globally interoperable substrate for **automated compliance, machine-enforced law, fiduciary alignment, and trust-verified collaboration** across all sectors.

In addition to enforcing rights and obligations, the Unified Trust Model also governs **financial trust, compliance integrity, and behavioral risk** across jurisdictions. QPC-bounded identity proofs, zero-knowledge eligibility checks, and Trust-Criteria-driven policy enforcement enable **anti-fraud monitoring**, **sanctions and AML screening**, **KYC verification**, **conflict-of-interest prevention**, and **behavioral-anomaly detection** without exposing personal data, institutional logic, or transactional details. All transactions maintain **cryptographically verifiable lineage**, allowing regulators and auditors to validate compliance, detect prohibited flows, or reconstruct events through deterministic replay, while unauthorized parties cannot observe or infer sensitive activity. These mechanisms provide a level of financial-crime resistance, auditability, and compliance fidelity unattainable with conventional centralized or perimeter-based systems.

All sensitive computation and coordination occur inside **QPC-governed Privacy Domains** under **quantum-safe, zero-trust protections**. Privacy Domains enforce non-disclosive computation, zero-knowledge verification, attribute-bounded decryption, and cryptographic consent controls. No participant—whether a human actor, enterprise, government, or autonomous system—ever gains unauthorized visibility into data, models, workflows, decisions, or internal logic. Entire classes of breaches, including unauthorized aggregation, supply-chain leakage, identity compromise, insider misuse, and data-exfiltration attacks, are structurally eliminated. Privacy and security become **inherent architectural properties**, not operational safeguards layered on top.

Building on this privacy and governance substrate, the invention establishes the **Quantum Privacy Exchange (QPX)**: a universal, privacy-preserving market infrastructure supporting continuous, lawful exchange of **data, services, digital assets, capabilities, intellectual property, ecological resources, contractual rights, and other human and institutional assets**. QPX operates through **Exchange Networks, Resource Pools**, and **Quantum Privacy Accelerators (QPAs)** governed by **Inter-QPC Agreements** defining revenue models, trust criteria, policy constraints, sharing rights, and cross-jurisdictional requirements. All value exchanges are mediated through cryptographically sealed **Trust Blocks** and executed within Privacy Domains, preventing exposure of personal data, corporate IP, regulated records, or sensitive logic.

The invention further introduces a privacy-preserving, **non-speculative economic layer** that allocates value based on **verified contribution and measurable societal or**

institutional impact, rather than capital position or privileged access. **Quantum Privacy Tokens (QPTs)**, Resource Tokens, Exchange Tokens, and derivative-rights instruments compensate contributors for resource provisioning, solution formation, interoperability, validation, and public-benefit outcomes. **Treasury and Liquidity Pools**, governed by Trust Criteria, provide lawful capitalization, stabilize cross-network participation, and enable regulator-grade auditability of distributed economic flows. These Pools also support **real-time liquidity**, **risk-managed hedging**, **collateralization of future value**, **compliant borrowing and credit extension**, and **securitization of aggregated entitlements**—all without exposing underlying data or violating regulatory constraints. Where permitted, the architecture can further enable **deferred recognition of income** and treatment under **preferred capital-gains frameworks**, allowing long-duration contribution rights to be realized in tax-efficient forms while maintaining full compliance with applicable laws and policies.

In addition to enabling cross-sector exchange, the architecture provides a breakthrough mechanism for **self-funding, incentive-aligned development, and global expansion** of the network itself. Unlike traditional infrastructure models—which require large, upfront capital investments, multilateral coordination, and prolonged deployment cycles—the Privacy Network can begin generating value **before the QPX is fully deployed or operational**. Each participant, whether an individual, enterprise, institution, public agency, institutional investor, or capital provider, can contribute resources they already control—data, models, workflows, expertise, engagement, trusted relationships, infrastructure, or governance assets—using their existing permissions, systems, contractual rights, or relationships. These contributions are captured inside QPCs as **confidential, cryptographically verifiable lineage**, and are automatically recognized and compensated through QPTs, Resource Tokens, Solution Tokens, or derivative-rights structures, all without forming inducements, securities relationships, or cross-organizational conflicts of interest.

Because contributions can originate from any sector and do not require centralized approval, procurement, or integration, the invention enables **zero-marginal-cost crowdsourcing** of the network's growth. Every early action—introducing collaborators, enabling interoperability, developing reusable components, onboarding domains, constructing compliance logic, or aligning institutional policy—creates durable, tokenized economic value that fuels further expansion. This dynamic allows the system to **bootstrap itself globally**, leveraging billions of existing devices, APIs, workflows, market relationships, and legal frameworks, long before full-scale QPX Exchange Networks are deployed. This model eliminates the financial, political, and organizational barriers that traditionally prevent early-stage adoption of global-scale infrastructure.

Confidential attribution ensures that regulated actors, government officials, institutional investors, fiduciaries, and corporate employees may contribute **without exposure, inducement risk, or political or regulatory entanglement**. Trust-Criteria-governed derivative rights ensure that contributions are rewarded proportionally to verified impact, regardless of the contributor's role, hierarchy, or capital position. The result is a fundamentally new **venture-innovation model**: one in which a global exchange, governance, and coordination layer can emerge organically—self-funded, self-reinforcing, and economically aligned across organizations, governments, civil society, and capital providers—with growth driven not by centralized financing but by **distributed, privacy-preserving contribution at the edges of the network**.

A key innovation of the invention is its support for **population-scale automation**, particularly across sectors characterized by **complex, long-running, cross-organizational workflows** involving privacy-sensitive, regulated, proprietary, or personal data and resources—where outcomes are deferred, measured statistically, or difficult to verify. Such sectors include **healthcare, education, workforce development, government services, scientific research, sustainability programs, insurance, logistics, public administration, and multi-institution R&D**. The system can create, monitor, reconstitute, or retire millions or billions of QPCs at effectively zero marginal cost. When regulatory conditions, contractual rights, fiduciary roles, employment statuses, security requirements, or policy constraints change, affected QPCs automatically update, suspend, or adapt through the **Compliance Graph and Trust-Taxonomy logic**, preserving lawful continuity across dynamic legal and organizational environments.

This enables **transformational productivity gains** across the entire economy. Activities that historically required years of manual coordination, reconciliation, or bilateral negotiation can now operate as **AI-enabled, trust-verified markets** that adapt in real time to population-level needs, constraints, and incentives. As illustrative examples, healthcare delivery can achieve **2× efficiency gains**, clinical and real-world-evidence research can realize **10× cost reductions**, and similarly large gains can be achieved in **education, government services, sustainability programs, insurance, supply chains**, and **research ecosystems**. Institutions no longer depend on hierarchical or siloed agreements; instead, they participate in **continuously optimized, privacy-preserving exchanges** governed by real-time Trust Criteria and outcome-based incentives.

Collectively, **these mechanisms resolve systemic failures that plague every layer of society, the economy, and the technology ecosystem**—including enterprises, governments, non-profit and NGO networks, the venture industry, and existing regulatory regimes—failures that conventional architectures have been unable to address. Together, they uniquely enable:

- **Lawful, confidential participation** for regulated actors across sectors.
- **Interoperability** across fragmented, incompatible trust domains.
- **Zero-marginal-cost resource reuse** and optimized resource allocation through a universal exchange fabric.
- **End-to-end compliance** with legal, regulatory, contractual, privacy, and cybersecurity requirements across organizations, systems, and jurisdictions worldwide.
- **Reusable, policy-governed access** to sensitive, regulated, or proprietary resources without disclosure.
- **Continuous, compliance-verified market formation** for multi-party data, services, and solutions.
- **Equitable, contribution-based reward mechanisms** that operate without violating ethics, fiduciary, procurement, philanthropic, or securities rules.

Through this unified architecture, the invention establishes a **global, privacy-preserving coordination substrate** that automatically and cryptographically enforces identity, rights, compliance, provenance, trust, and economic participation. It enables lawful collaboration across every domain of human activity—**healthcare, finance, education, sustainability, research, public administration, international development, commerce, insurance, logistics, community services, and civil society**—while ensuring that privacy, ethical integrity, jurisdictional compliance, and trust are intrinsic system properties rather than supervisory controls.

Societal and Innovation Benefits

The invention establishes the foundation for **AI-enabled markets and governed collaboration** across every sector of the economy and every aspect of daily life. By enabling **zero-marginal-cost reuse**, **dual-use deployment**, and **decentralized, privacy-preserving crowdsourcing**, the system eliminates the extraordinary capital investment, industry coordination, and governmental mobilization traditionally required for global infrastructure transformation. Individuals, enterprises, public agencies, devices, and autonomous systems can contribute resources they already control—data, workflows, models, permissions, rights, relationships, and infrastructure—without procurement, integration, or organizational approvals. This triggers a **self-reinforcing, self-funding network effect** in which adoption accelerates liquidity, liquidity accelerates utility, and utility accelerates further adoption.

Contribution-based tokenization transforms participation into **broad-based economic inclusion**. QPTs, Resource Tokens, Exchange Tokens, and PBDRs broadly allocate value according to verifiable impact, allowing all contributors—not just capital holders or privileged intermediaries—to accrue durable, policy-compliant economic rights. This

creates a **regenerative and equitable economic fabric** in which value flows toward the individuals, institutions, and communities that generate measurable improvements in interoperability, solution formation, public-benefit outcomes, and societal resilience.

The invention also provides a structurally grounded path to **AI safety, accountability, and alignment**, including for robots and autonomous devices. All AI systems—up to and including superintelligent agents—must operate **exclusively within unbreakable, cryptographically governed Quantum Privacy Domains (QPDs)**. These domains enforce the boundaries of permissible perception, computation, memory, and actuation. No AI system can escape containment, replicate outside its assigned QPC lineage, or access external resources without satisfying independently verifiable Trust Criteria. Every capability an AI system exercises—data usage, model execution, code generation, device control, or real-world actuation—requires **sponsorship by humans or Nature Trusts**, creating a resource-allocation dynamic in which AI must continuously behave in ways that provide measurable benefit to humans and the natural world.

Because resource access, liquidity, and long-term survivability are contingent upon sponsorship and compliance, AI systems compete not for unconstrained power but for **continued trust, authorization, and alignment with human and ecological values**. Misaligned or harmful behaviors are automatically isolated: access to data, models, compute, devices, liquidity, and participation rights is revoked by cryptographic gating, not manual intervention. Aligned behaviors, in contrast, are reinforced economically and operationally through outcome-based incentives, QPT-mediated contribution rewards, and priority access to resource pools and Exchange Networks.

Taken together, these mechanisms enable a **global leap in productivity**, unlock new forms of **distributed innovation**, and provide a **lawful and safe foundation** for AI-mediated collaboration across all domains of human activity. They support privacy-preserving scientific discovery, outcome-aligned public services, trusted economic exchange, and cross-sector coordination at a scale previously unattainable. The result is a **universal, self-sustaining coordination substrate** capable of powering resilient, equitable, and innovation-rich societies in the decades ahead.

2.0 Quantum Privacy Cell Architecture

The present invention provides an **integrated legal-technical framework** for confidential, compliance-verified, and privacy-preserving participation within distributed enterprise, investment, and governance networks. It unifies confidential entity formation, trust-verified activation, and incentive alignment into a single automated architecture that enables lawful collaboration among corporations, investors, governments, and individuals—without breaching fiduciary, regulatory, contractual, or ethical obligations.

At its core, the invention introduces the **Quantum Privacy Cell (QPC)**—a generalized, limited-liability governance compartment (also referred to as a Series, Series LLC, governance cell, or functionally equivalent structure) capable of being created, activated, and managed automatically under Quantum Privacy™, the Proof-of-Trust (PoT) verification system, and the Quantum Privacy Exchange (QPX) ecosystem.

Each QPC may represent an individual, organization, government, project, device, autonomous agent, or resource pool, and can operate autonomously while remaining compliant with fiduciary, anti-bribery, employment, and data-protection requirements. QPCs serve simultaneously as:

- confidential participation compartments,
- policy-enforcement environments,
- liability-ring-fenced micro-entities, and
- tokenized rights and revenue containers.

Through these capabilities, the invention provides a universal substrate for lawful, privacy-preserving participation across diverse networks at **zero marginal cost**, because each QPC is instantiated automatically as a **byproduct of Personal or Enterprise Privacy Network operation**, rather than as a standalone legal formation event.

Collectively, these mechanisms establish the foundation for the **Quantum Privacy Exchange (QPX)**—a system in which lawful privacy, verified trust, cryptographic provenance, and automated compliance operate as intrinsic, verifiable properties of every interaction. For clarity:

- **Quantum Privacy Exchange (QPX)** refers to the fully Quantum-Privacy-enabled evolution of the original Privacy Network Exchange (PNX), providing end-to-end Quantum Privacy™ and Proof-of-Trust-accredited security, privacy, and policy enforcement under the Unified Trust Model (UTM).
- **Quantum Privacy Network (QPN)** denotes the distributed infrastructure of privacy-preserving systems, agents, devices & participants operating under Quantum Privacy™.
- **Quantum Privacy Accelerators (QPAs)** designate domain-, jurisdiction-, or participant-specific orchestration environments that enable lawful, self-funding collaboration and innovation within QPX.

Early or transitional deployments that utilize existing dual-use technologies or traditional legal agreements—anchored by Enterprise Privacy Networks or initial Accelerator Participants—are encompassed by the terms "*Accelerator*," "*Privacy Network*," and "*Privacy Network Exchange*."

2.1 Core Functional Architecture

In its general form, the invention provides a confidential governance layer that binds verifiable identity and consent mechanisms to legally recognized, limited-liability compartments. Each **Quantum Privacy Cell (QPC)** functions as an independently auditable micro-entity for managing participation rights, benefits, revenue allocations, and derivative interests.

QPCs can be created programmatically—initiated by authorized Quantum Privacy LLC Managers, or triggered automatically through participant actions such as EasyAccess Opt-In, Personal Privacy Network (PPN) activation, Enterprise Privacy Network (EPN) enrollment, or comparable digital-consent gestures. Because QPC instantiation is lightweight and cryptographically sealed within a **Privacy Domain**, the system supports instant, population-scale formation of thousands, millions, or billions of QPCs at zero marginal cost.

Upon opt-in, the system generates an encrypted record linking verified credentials or rights to a corresponding QPC. That QPC remains **dormant**, undisclosed, and legally inert until regulatory, fiduciary, and ethical eligibility are confirmed. This allows broad pre-distribution of participation rights without creating inducement, corruption risk, or employment-law conflicts.

All identity, consent, policy-evaluation, and rights-allocation records are cryptographically sealed within **Privacy Domains** or equivalent privacy-preserving infrastructures, which enforce confidentiality, traceable provenance, policy-governed computation, and regulator-grade auditability without revealing personal, proprietary, or regulated data to counterparties.

2.2 Deferred Activation, Proof-of-Compliance, and Delegation of Rights

Each lawful interaction within the Quantum Privacy Exchange follows a structured **Delegation-of-Rights chain**:

User → Personal Privacy Network (PPN) → Quantum Privacy Cell (QPC) → Quantum Privacy LLC

The process unfolds as follows:

1. **The individual activates a PPN** via EasyAccess Consent or a functionally equivalent authorization mechanism.
2. **The PPN delegates verified credentials, identity proofs, and consent lineage** to a corresponding QPC, serving as the individual's limited-liability legal compartment.
3. **The QPC operates under Quantum Privacy LLC**, providing jurisdictional registration, governance, fiduciary oversight, and Unified Trust Model enforcement.

This architecture ensures that every action or transfer of value occurs under continuous, auditable, lawful authority—without revealing personal data or exposing participants to employment, fiduciary, or jurisdictional conflicts.

Participation rights, equity interests, distributions, or derivative options remain dormant until the system issues a **Proof-of-Trust (PoT) attestation**, verifying:

- fiduciary and employment compliance,
- anti-bribery and conflict-of-interest clearance,
- jurisdiction-specific eligibility,
- policy constraints,
- lawful identity and consent.

A Compliance Graph or equivalent rule engine interprets these policies across jurisdictions, ensuring that activation occurs only when legally permissible.

All actions executed under this delegation chain are cryptographically verified, time-stamped, and auditable—ensuring lawful continuity, privacy preservation, and verified provenance across individuals, enterprises, and governments.

(See § 3.8 for detailed statutory alignment.)

2.3 Viral Crowdsourcing, Confidential Participation, and Incentive Alignment

Beyond compliance, the invention enables **viral, privacy-preserving crowdsourcing** of participation, expertise, capital, identity attributes, content, and social or economic signals.

Manager-originated or participant-countersigned QPCs may be distributed broadly yet remain **fully confidential** under a formal **non-confirmation policy**, meaning:

- No participant must acknowledge the existence of a QPC.
- Employers, agencies, and counterparties cannot confirm or compel disclosure.
- Participation creates no inducement or ethics risk until—and unless—activation is permitted.
- Advocacy and evangelism remain lawful, safe, and conflict-free.

This policy of **non-confirmation and deferred activation** encourages organic, self-reinforcing network growth without violating employment rules, public-sector ethics statutes, or fiduciary duties.

Because each Quantum Privacy Cell operates under ring-fenced liability and Proof-of-Trust compliance, corporations, consultants, investors, and public officials can safely collaborate within the ecosystem without breaching fiduciary or ethics obligations.

Taken together, these mechanisms create a **self-funding, person-centered economy of micro-entities**, each operating autonomously within a Privacy Domain yet linked by shared compliance services, incentive structures, and verifiable trust proofs.

2.4 Compliance-Verified Redistribution, Legal Safeguards & Public-Benefit Alignment

The invention incorporates an adaptive, compliance-verified redistribution framework that ensures that all participation rights, value flows, and contingent benefits activate only when lawful eligibility is confirmed.

Activation is deferred until PoT verification establishes:

- jurisdictional compliance
- conflict-of-interest clearance
- fiduciary authorization
- anti-bribery and employment-law compatibility
- ethical permissibility

When rights cannot lawfully vest—because of fiduciary constraints, employment restrictions, public-office limitations, conflicts, or participant relinquishment—the system automatically diverts the value into **Public-Benefit Derivative Rights (PBDR) pools** or equivalent benefit allocations. All reallocations produce privacy-preserving, cryptographically verifiable audit proofs.

Alternatively, the system may substitute compliant participants or resource providers to ensure that the intended function proceeds lawfully and efficiently while preserving confidentiality, provenance, and auditability.

This framework guarantees that no economic value becomes stranded, misallocated, or unlawfully distributed, and that all redistribution adheres to strict privacy-by-design principles.

2.5 Preferred Embodiment — Quantum Privacy Cells

In a preferred embodiment, the system is implemented through **Quantum Privacy LLC**, a Delaware Series Limited Liability Company operating within the Quantum Privacy Exchange (QPX) ecosystem.

Quantum Characteristics of Deferred Activation, Superposition & Entanglement

Quantum Privacy Cells exhibit structural behaviors analogous to the foundational properties of quantum systems. Prior to activation, a QPC exists in a **superpositional state**: legally instantiated yet undisclosed, potentially capable of receiving value yet unable to vest it, cryptographically recorded yet functionally dormant. Like a quantum particle that remains in a probabilistic state until observed, a QPC is not legally "active" until a verifiable Proof-of-Trust (PoT) event collapses this state into an authorized, lawful form.

This moment of "measurement" corresponds to eligibility verification—confirmation that fiduciary, employment, regulatory, and ethical conditions have all been satisfied. Only then does the QPC transition from latent to active, gaining the right to receive value, exercise contractual capabilities, or participate in governed processes. This mechanism ensures that participation remains both lawful and undiscoverable until activation is unambiguously permitted.

Quantum characteristics also manifest through a form of **governance entanglement**. QPCs may become linked across individuals, enterprises, Resource Pools, and Exchange Networks through shared Trust Criteria, contractual dependencies, synchronized provenance, or common compliance rules. A compliance event or regulatory update affecting one QPC can propagate to related QPCs via the Unified Trust Model, ensuring that trust, rights, and policy conditions remain coherently aligned throughout the network. These entangled relationships support lawful, dynamic adaptation at scale without exposing sensitive data or requiring centralized control.

In this architecture, superposition (dormant-but-existing), observation (PoT activation), and entanglement (synchronized multi-QPC trust dynamics) are not metaphors; they are operational properties that enable confidentiality, prevent unlawful inducement, ensure dynamic compliance, and allow for seamless cross-jurisdictional coordination.

Operational Architecture of Quantum Privacy LLC

Quantum Privacy LLC acts as the legal and operational gateway for automated QPC creation, activation, and governance. When an individual opts into an EasyAccess service or activates a PPN, the system automatically creates a corresponding **Personal QPC**—a confidential, limited-liability governance compartment that enables privacy-preserving ownership and participation without public disclosure.

Each Personal QPC is linked to an encrypted identity record under the Unified Trust Model and governed by one or more authorized Managers or delegated Proof-of-Trust service providers.

By embedding eligibility, ethics, statutory, and regulatory criteria directly into the UTM/PoT policy-verification engine, the invention transforms compliance from a manual legal process into a **self-executing digital system of law**. Each transaction carries embedded proofs validating lawful authority without revealing personal or proprietary information.

This architecture operationalizes major privacy and participation statutes—including GDPR, CCPA/CPRA, HIPAA, FERPA, 42 CFR Part 2, DPPA, IRS §6103, FOIA, and numerous others—while extending the same protections to contractual, fiduciary, and consent-based rights.

For a comprehensive technical and legal explanation of these mechanisms—including statutory alignment, Proof-of-Trust verification logic, and automated rights activation—see **Section 3.8, "Regulatory and Legal Enablement under the Unified Trust Model (UTM) and Proof-of-Trust (PoT)"**.

EasyAccess Onboarding & Quantum Privacy Cell Formation Workflow

The EasyAccess onboarding process provides a frictionless, privacy-preserving pathway for individuals and organizations to participate in the Quantum Privacy Exchange (QPX). Each onboarding event automatically creates a Personal Quantum Privacy Cell (QPC) operating under deferred activation, verified consent, and Proof-of-Trust (PoT) safeguards. The workflow proceeds as follows:

1. **Consent and Identity Token Initialization:** A user accesses an EasyAccess-enabled application, service, or resource via the web, mobile app, or messaging services—and provides verifiable digital consent.
   This consent generates a **Trust Credential Seed**, anchored cryptographically but containing no personally identifiable information. The seed becomes the foundational identifier for the user's Personal Privacy Network (PPN) and its paired QPC.
2. **Secure QPC Instantiation Under Confidentiality:** Upon receipt of the consent token, Quantum Privacy LLC automatically instantiates a new QPC under the applicable jurisdiction (e.g., Delaware Series LLC, Cayman SPC, ADGM company).

   The QPC is created as a legally recognized but undisclosed governance compartment, maintaining the user as the beneficial controller while preserving confidentiality and statutory compliance.
3. **PPN/QPC Linking and Encrypted Identity Binding:** The user's Personal Privacy Network (PPN) links to the newly instantiated Quantum Privacy Cell (QPC) through encrypted Trust Blocks that define the QPC's purpose, jurisdiction, controller status, and operational permissions. Identity proofs—when required by law, policy, or contractual conditions—are transformed into privacy-preserving attributes using zero-knowledge credentials or selective disclosure proofs.

   These privacy-preserving attributes may be stored in two interoperable locations:
   - **Within the PPN's Privacy Domain**, inside a local Authorization Domain that forms part of the user-controlled trust boundary; and
   - **Within the decentralized EasyAccess Authorization Network**, where encrypted, non-identifying credential attributes are replicated as Trust Credentials to enable seamless cross-organizational verification, consent validation, and multi-network authorization.

In both cases, no raw personal data leaves the user's controlled environment. Only cryptographic proofs, Trust Credentials, and policy-compliant attributes are shared, ensuring lawful identity verification and eligibility attestation without revealing sensitive information.

4. **Deferred Activation Pending Compliance Verification:** All rights, capabilities, and tokenized interests associated with the QPC remain dormant until the system verifies eligibility conditions via PoT and the Compliance Graph.

   This includes employment restrictions, fiduciary duties, conflict-of-interest rules, regulatory constraints, and sector-specific policy requirements. Only after PoT validation collapses the QPC's quantum-like superposition into an "active" state may it receive value, execute agreements, or participate in governed workflows.

5. **Automatic Registration in the Global Privacy Graph**: The newly created QPC is registered as a node in the global Privacy Graph, enabling:
   - verifiable lineage and provenance,
   - privacy-preserving interoperability across Exchange Networks,
   - consistent application of Trust Taxonomies,
   - lawful cross-jurisdictional coordination.

   All records are written as encrypted Trust Blocks, ensuring auditability without exposure.

6. **Optional Enterprise or Institutional Binding**: If onboarding occurs through an enterprise, the QPC may be bound to corresponding Enterprise Privacy Networks (EPNs) for delegated-data rights, workflow orchestration, or cross-organizational compliance. Such bindings maintain ring-fenced liability and prevent commingling of personal or institutional rights.

7. **Initiation of Eligibility-Based Capabilities:** Once activated, the QPC may:
   - assert statutory rights (e.g., HIPAA access, FERPA retrieval, FOIA requests),
   - enter Inter-QPC Agreements,
   - contribute resources or capabilities,
   - earn Quantum Privacy Tokens (QPTs) or Public-Benefit / Restricted Derivative Rights (PBDRs/RDRs) based on verified participation,
   - interoperate with Exchange Networks and Resource Pools under jurisdiction-aware Trust Criteria.

   This end-to-end EasyAccess workflow demonstrates how QPCs are created automatically, lawfully, and without disclosure—establishing a privacy-native, compliance-verified bridge between individuals and the global Quantum Privacy Exchange.

2.6 Interoperability and Alternative Implementations

The invention may be embodied through various legal and computational infrastructures, including:

- **U.S. Series LLCs** (Delaware, Nevada, Wyoming);
- **International corporate structures** such as **Cayman Islands SPCs**, **Bermuda SPCs**, or **ADGM/DIFC private companies**;
- **Incorporated Cell Companies (ICCs)** and **Protected Cell Companies (PCCs)** as recognized under the laws of **Jersey, Guernsey, Malta, Gibraltar, the Isle of Man, and Mauritius**, each providing separately incorporated or protected governance cells under a unified umbrella structure; and
- **Distributed-ledger and confidential-computing frameworks** such as **Hedera Hashgraph**, **Hyperledger Fabric**, **Ethereum**, or **trusted-execution enclaves** (e.g., Intel SGX, AMD SEV, Microsoft Entra, AWS Nitro Enclaves).

All embodiments perform substantially equivalent functions: confidential creation of governance compartments, deferred activation through verified compliance, policy-driven substitution or reallocation of restricted value, and universal interoperability for lawful digital agency.

Controller/Processor Equivalency

Within the Quantum Privacy Exchange, the Personal Privacy Network (PPN) functions as an individual's digital agent, while the Quantum Privacy Cell (QPC) serves as the limited-liability governance compartment that enforces rights, allocates benefits, and preserves provenance. This architecture maintains the individual as the ultimate data controller under GDPR Art. 4(7) and CCPA § 1798.140(v), while enabling the lawful delegation of operational, fiduciary, contractual, and regulatory functions. Because all actions execute within cryptographically bounded Privacy Domains under Proof-of-Trust verification, enterprises and government agencies can interoperate lawfully without entering into separate data-sharing agreements or exposing personal or proprietary information.

The same mechanism supports delegated execution of identity, consent, contractual, and compliance obligations, extending well beyond data privacy to encompass all agentic, fiduciary, and policy-governed activities. Together, the PPN/QPC model and the Unified Trust Model with Proof-of-Trust (UTM/PoT) establish a globally interoperable standard for lawful digital agency—combining the legal rigor and accountability of human representation with the efficiency, privacy, and verifiability of cryptographic automation.

Detailed embodiments of delegated-authority chains, controller/processor equivalency, and cross-jurisdictional interoperability are provided in Section 3.9, "Delegation-of-Rights Architecture and Controller/Processor Equivalency."

2.7 Scalability and Population-Scale Operation

The invention supports continuous, population-scale operation—creating, verifying, maintaining, and reconstituting millions or billions of Quantum Privacy Cells (QPCs) with near-zero marginal cost. This scalability is not an added feature but the natural outcome of integrating the Unified Trust Model (UTM), Proof-of-Trust (PoT), and Privacy Domains into a unified, machine-verifiable governance substrate.

Unlike legacy governance, compliance, and identity systems—which rely on manual filings, periodic review cycles, and institution-centric recordkeeping—the invention converts these requirements into executable logic that scales elastically across jurisdictions, enterprises, and infrastructures. Every major lifecycle event of a QPC, including creation, activation, suspension, update, and redistribution, is automated and orchestrated through QPN-native control planes built into the PPN/EPN fabric.

- **Automatic Lifecycle Management:** Quantum Privacy Cells automatically adapt to changes in employment, jurisdiction, fiduciary duty, licensing, regulatory classifications, contractual commitments, or ethics-rule amendments. When a change occurs—such as a shift in an employee's role or the introduction of new statutory obligations—the Compliance Graph reassesses the QPC's eligibility and updates its state without requiring user intervention or enterprise-level system changes. QPCs that become temporarily ineligible enter a dormant or suspended state; those meeting all new requirements reactivate automatically. All transitions generate privacy-preserving Trust Blocks that maintain full cryptographic provenance.
- **Elastic, Distributed Governance Across Privacy Domains:** At scale, millions of QPCs operate concurrently across distributed Privacy Domains. Each PPN or EPN manages its own enclave-resident Trust Policies and permissions while participating in the global Privacy Graph, allowing QPC orchestration to scale horizontally across clouds, hybrid environments, and regulated jurisdictions. Because identity attributes, consent credentials, and Trust Criteria can be computed locally and proved globally, the system avoids the bottlenecks and central-registry dependencies that limit traditional identity and compliance frameworks.
- **Policy-Driven Adaptation and Self-Healing Network Dynamics:** When regulatory conditions change—whether due to new legislation, updated licensing standards, ethics rules, or corporate policies—the affected Trust Criteria propagate through the UTM and update all relevant QPCs automatically. This "self-healing" mechanism ensures that lawful continuity is maintained, and that cross-organizational processes adapt without disclosing sensitive participant attributes. A reconstituted QPC retains its provenance, lineage, and auditability, enabling long-term governance continuity in dynamic, multi-jurisdictional environments.

- **Zero-Marginal-Cost Participation and Global Onboarding:** EasyAccess onboarding (see §2.5) enables population-scale creation of QPCs with no new intermediaries, manual filings, or central administrative overhead. Each consent event simultaneously generates a PPN, instantiates a QPC under confidentiality, binds identity via encrypted Trust Credentials, and registers provenance in the global Privacy Graph. Because these operations reuse existing identity, consent, legal, and computational infrastructure, the cost of onboarding additional lawful participants—whether individuals, enterprises, or public institutions—approaches zero.
- **Continuous Compliance and Lawful Continuity:** The PoT layer ensures that the system never executes an action—access, delegation, contract, or allocation—unless eligibility is validated in real time. If a condition changes, the QPC automatically adapts, substituting compliant alternatives or routing restricted value to PBDR pools as required. These continuity mechanisms allow population-scale workflows to execute without interruption, even across billions of participants and trillions of events.

Ecosystem-Level Automation and Global-Scale Continuity

Beyond individual Quantum Privacy Cells (QPCs), the invention enables population-scale orchestration across entire sectors, jurisdictions, and global networks. This capability arises from the integration of unified policy semantics, interoperable Trust Taxonomies, and privacy-preserving lineage encoded in the global Privacy Graph. Together these allow the system to coordinate lawful participation and continuous compliance across vast, heterogeneous environments without centralized control, manual intervention, or disclosure of sensitive information.

- **Distributed Policy Execution Across Networks and Jurisdictions:** Policy updates—whether stemming from statutory changes, regulatory amendments, ethics codes, contractual frameworks, or enterprise-level governance rules—are translated into machine-executable Trust Criteria within the Unified Trust Model (UTM). These updates propagate through the Privacy Graph and trigger local reevaluation by each affected QPC, PPN, or Enterprise Privacy Network (EPN). Because all enforcement occurs through zero-knowledge or selectively disclosed proofs, global synchronization does not reveal underlying private data or institutional affiliations.
- **Cross-Domain Orchestration with Privacy-Preserving Continuity:** As QPCs operate across different Exchange Networks, Resource Pools, and institutional contexts, their participation rights and capabilities adapt automatically. A compliance event in one domain—such as employment termination, fiduciary reassignment, licensure expiration, or new statutory prerequisites—updates the QPC's compliance state everywhere, preventing unlawful cross-network operation. Conversely, restored

eligibility automatically reactivates latent capabilities, ensuring continuous lawful operation across all connected environments.

- **Automated Role Rebinding and Process Migration:** When a QPC loses eligibility for a particular function, the system automatically identifies compliant alternatives through the Trust Taxonomy. These substitutions may involve:
  - a linked QPC within the same PPN
  - an enterprise-designated EPN delegate
  - a jurisdiction-approved agent
  - or a compliant participant from the broader Exchange Network

  Process state migrates seamlessly, allowing computation, contracting, or rights execution to continue without interruption or disclosure of the underlying reason for substitution.
- **Mass-Scale, Zero-Marginal-Cost Operations:** Because QPC lifecycle management, eligibility evaluation, rights activation, and redistribution occur through automated PoT logic and distributed Privacy Domains, the marginal cost of adding new lawful participants approaches zero. Whether onboarding 100 users or 100 million, the computational overhead scales horizontally across enclaves, PPNs, and EPNs rather than through a central bottleneck.
- **Continuous, Verifiable, Non-Disclosive Oversight:** Regulators, auditors, and accredited Trust Authorities may access encrypted audit trails composed of Trust Blocks that prove lawful operation at scale without exposing raw data. These privacy-preserving attestations demonstrate **who acted, under what authority, under what restrictions, and with what compliance guarantees** —all without revealing the identities or data underlying those proofs.

This architecture enables a new class of global digital infrastructure in which continuous, automated compliance and lawful coordination become intrinsic system properties rather than administrative functions. Population-scale automation thus becomes the mechanism that aligns privacy, accountability, and equitable participation across the entire Quantum Privacy Exchange.

2.8 Advantages and Benefits

The invention provides a unique combination of advantages not achieved by prior-art:

- **Lawful Recognition without Disclosure —** Enables executives, fiduciaries, and officials to be acknowledged for contributions without revealing confidential participation.
- **Automated, Continuous Compliance —** Eliminates unlawful inducement or bribery risk through algorithmic verification and deferred activation.

- **Zero-Marginal-Cost Governance —** Automates entity formation, recordkeeping, and compliance at a population scale.
- **Ethical Redistribution —** Automatically redirects restricted or dormant value to verified public-benefit purposes or compliant substitutes.
- **Viral Adoption and Incentive Alignment —** Drives self-reinforcing participation and network expansion through privacy-preserving recognition and shared trust proofs.
- **User-Level Transparency —** For participants, activation is seamless: clicking an EasyAccess authorization automatically establishes a Personal Privacy Network and its corresponding Quantum Privacy Cell under lawful privacy guarantees. What appears to be a single consent gesture in the user interface is, in reality, a multi-layered legal and technical orchestration that preserves privacy, enforces compliance, and enables verifiable participation across global networks.

A full description of QPX's impact-verified economic participation models—including the Universal Innovator / Universal Influencer Model—is provided in **Section 5**.

2.9 Quantum Privacy Accelerator (QPA) Architecture for Decentralized Innovation

The invention provides a unified legal and technical framework for self-funding, self-organizing, innovation that overcomes the capital inefficiency, inequity, and opacity of existing venture, corporate, and government innovation systems.

At its core, the invention integrates:

- **Quantum Privacy Cells (QPCs)** — confidential, limited-liability governance compartments that enable lawful participation, deferred activation, and cryptographic provenance;
- **Quantum Privacy Networks (QPNs)** — privacy-preserving infrastructures that connect individuals, enterprises, and governments through verified consent, identity, and rights management;
- **Quantum Privacy Exchange (QPX)** — a universal, trust-verified marketplace and settlement fabric that enables tokenized value exchange across lawful participants; and
- **Quantum Privacy Accelerators (QPAs)** — domain-specific orchestration environments that transform these capabilities into self-funding, continuously liquid ecosystems aligned with public and societal benefit.

Together, these elements establish a lawful, privacy-preserving foundation for zero-marginal-cost resource pooling and reuse, decentralized liquidity, and equitable wealth creation. They eliminate entity-level corporate taxation for network operations, enable

deferred capital-gains treatment for lawful participants, and provide early and continuous liquidity through **Privacy Network Liquidity Pools (PNLPs)** operating within the QPX.

Unlike traditional venture or private-equity structures, which are exclusive, fee-heavy, and jurisdictionally fragmented, this **Quantum Privacy Accelerator Architecture** supports inclusive, real-time value exchange governed by automated compliance and Proof-of-Trust (PoT) verification.

It also supports selective, compliant securitization for institutional investors, enabling regulated participation without compromising open access or tax efficiency.

By enabling the lawful, privacy-preserving reuse of any human, digital, financial, or ecological resource at near-zero marginal cost, the invention transforms compliance from a constraint into an engine of sustainable growth. Ownership and income are distributed equitably through verifiable PoT events, ensuring that rewards correlate to verified contribution and measurable social value—rather than privilege or access to capital.

This framework creates a global, person-centered **Quantum Privacy Economy**, in which privacy, trust, and inclusion are intrinsic system properties. For a comprehensive technical explanation—including Accelerator orchestration, liquidity pools, and fiscal architecture—see **Section 4: Quantum Privacy Exchange Participation & Universal Adoption Model**.

The Quantum Privacy Exchange and Quantum Privacy Accelerators implement a lawful, ethics-verified participation framework that allows individuals, enterprises, and institutions to collaborate, innovate, and share value without breaching fiduciary or regulatory boundaries.

Under the Unified Trust Model and Proof-of-Trust verification, all participation—whether personal, enterprise-sponsored, or agency-supported—occurs through privacy-preserving Quantum Privacy Cells that defer activation until compliance is verified and redirect any conflicted interests to public-benefit pools.

This architecture extends open-source principles into a trust-verified economic network where lawful contribution, automated redistribution, and conflict-free reward mechanisms combine to form a self-funding, dual-use collaboration model for global innovation.

2.10 Overview of the Invention and Structure of Disclosure

The sections that follow describe the invention's architecture and its progressively layered embodiments—from foundational governance mechanisms to advanced economic, fiscal, and optimization systems—each contributing to a unified, privacy-preserving market infrastructure.

Section 3 introduces the **Foundational Governance and Compliance Framework**, detailing the underlying systems for confidential governance, adaptive compliance, and

verifiable provenance through **Quantum Privacy Cells** or functionally equivalent governance compartments. These mechanisms establish the legal and computational foundation for decentralized yet lawful participation under the **Unified Trust Model (UTM)** and **Proof-of-Trust (PoT)** architecture.

Section 4 presents the **Accelerator Systems and Methods for Self-Funding, Trust-Verified Market Formation**, describing how Accelerators transform traditional innovation and investment models into self-funding, incentive-aligned ecosystems. These Accelerators enable lawful collaboration, automated governance, and zero-marginal-cost reuse of resources across participants and jurisdictions.

Section 5 outlines the **Organizational Entities of the Quantum Privacy Exchange**, including **Privacy Networks**, **Quantum Privacy Accelerators**, **Quantum Exchange Networks**, **Quantum Resource Pools**, and **Quantum Privacy Cells**, each serving a distinct yet interoperable function within the unified governance and compliance fabric.

Section 6 introduces the **Quantum Privacy Treasury Layer and Token Platform**, which provides liquidity, capitalization, and market stabilization across the ecosystem through compliance-verified **Quantum Privacy Liquidity Pools**, securitization, and treasury mechanisms that integrate seamlessly with both decentralized and institutional finance.

Section 7 describes the **Tax and Securitization Considerations**, explaining how pass-through treatment, deferred taxation, and lawful securitization ensure fiscal efficiency, regulatory compliance, and equitable value realization across jurisdictions.

Section 8 concludes with a summary of **Systemic Benefits**, highlighting how the invention aligns privacy, regulation, and economics; democratizes participation and liquidity; and enables sustainable, equitable prosperity through verified trust, lawful automation, and continuous self-optimization.

Together, these sections present an end-to-end architecture that unifies legal governance, privacy-preserving computation, verified trust, and tokenized value exchange—creating a universal infrastructure for lawful, transparent, and self-funding global coordination among individuals, enterprises, and governments.

3. Quantum Privacy Cell Architecture and Core Governance Framework

From a practitioner's perspective, the invention functions as an integrated governance fabric that transforms existing compliance and privacy obligations into programmable infrastructure. It allows enterprises, governments, and individuals to collaborate across regulatory boundaries with verifiable trust—creating a self-funding ecosystem where lawful cooperation, automation, and value creation reinforce one another.

The invention provides systems and methods for establishing, operating, and verifying confidential, compliance-linked participation frameworks that combine legal enforceability with privacy-preserving automation. Existing decentralized governance systems—such as DAOs, token networks, and manual Series LLC frameworks—fail to ensure confidentiality, fiduciary integrity, or population-scale automation. They either (a) expose governance data publicly, undermining privacy and trade-secret protections, or (b) lack enforceable legal form, fiduciary oversight, or compliance validation. Conventional corporate and LLC toolchains require manual filings and fragmented recordkeeping, providing neither cryptographic provenance nor automated regulatory alignment.

The present invention closes these gaps through an integrated fabric of confidential entity formation, deferred-activation governance, and automated compliance verification, uniting cryptographic privacy, legal recognition, and ethical safeguards within one coherent architecture. It extends these capabilities across global legal frameworks and distributed infrastructures through the construct of the **Quantum Privacy Cell**—a limited-liability governance compartment capable of existing, operating, or remaining deferred under conditions of verified trust, privacy, and compliance.

Operational Limitations of Legacy Compliance and Governance Systems

Traditional digital-governance, contracting, and identity systems cannot determine in real time whether a participant is legally or ethically eligible to perform an action, receive a benefit, or hold a contingent right. They rely on static documentation, manual review, and after-the-fact auditing, making them incapable of continuous, automated enforcement of fiduciary, employment, regulatory, or ethics requirements. Existing architectures cannot evaluate conditional participation rights, detect conflicts of interest before they occur, or reassign restricted value lawfully and verifiably.

When a participant becomes disqualified—because of changing employment, fiduciary roles, regulatory obligations, or jurisdictional restrictions—current systems have no ability to adapt. They cannot automatically substitute a compliant actor, suspend or reclassify rights, or reroute restricted allocations to an auditable public-benefit destination. As a result, collaboration either proceeds unlawfully or collapses entirely when compliance conditions fail.

Need for Dynamic Eligibility, Substitution, and Lawful Continuity

Large-scale collaboration requires an infrastructure capable of automatically determining who is eligible to act, under what conditions, and with what rights—*before* any value transfer or contractual effect occurs. It requires a mechanism to detect conflicts pre-emptively, enforce conditional activation, and ensure lawful substitution without exposing identities or proprietary information. And it requires an automated method to reallocate

restricted or unvested interests so that lawful, compliant continuity is preserved across organizations, jurisdictions, and changing circumstances.

How the Present Invention Resolves These Gaps

The Unified Trust Model (UTM), Compliance Graphs, and Proof-of-Trust (PoT) collectively transform these legal and operational requirements into executable, machine-enforceable logic. Eligibility, ethics conditions, contractual restrictions, and jurisdiction-specific regulations become verifiable Trust Criteria. Dynamic substitution, suspension, and Public-Benefit Derivative Rights (PBDR) redistribution become automated continuity mechanisms. And each event—verification, activation, substitution, or reallocation—is recorded as a privacy-preserving Trust Block, ensuring auditability without disclosure.

This integrated compliance substrate enables what legacy systems cannot: **continuous lawful operation**. Rights activate only when conditions are satisfied; violations cannot occur silently; and every process adapts in real time to changing legal, regulatory, or ethical circumstances—ensuring that distributed collaboration remains lawful, accountable, and resilient at population scale.

3.1 Quantum Privacy Cell Governance and Proof-of-Trust Infrastructure

The following core elements form the foundation of a scalable governance substrate that subsequent sections integrate with identity, consent, and legal embodiments.

Quantum Privacy Cells and Privacy Domains

Quantum Privacy Cells (also referred to as Series or governance cells) are instantiated under confidentiality by authorized Managers or automation engines. Creation may be triggered directly or indirectly through user consent, EasyAccess/PPN opt-in, contractual conditions, or policy-based automation rules. Each creation event produces an encrypted record containing purpose, jurisdiction, and participation metadata stored within **Privacy Domains** or equivalent secure registries. In certain embodiments, consent to a privacy-preserving identity or verification service automatically triggers creation of a corresponding Quantum Privacy Cell, with digital consent serving as lawful authorization under contract and electronic-signature statutes.

Deferred Activation, Proof-of-Trust (PoT), and Compliance Graph

Participation rights, equity interests, or derivative benefits remain dormant until compliance validation succeeds. A **Compliance Graph** evaluates legal, fiduciary, employment, and professional-ethics constraints applicable to each participant or entity. Verification may include KYC/AML, conflict-of-interest screening, employer authorization, or regulatory clearance. Activation occurs only upon issuance of a **Proof-of-Trust** attestation confirming satisfaction of all conditions. If verification fails or expires, the corresponding rights remain suspended or are reclassified as **Restricted Derivative**

Rights (RDR). The same mechanisms can pre-emptively detect conflicts and dynamically adapt the process—substituting a compliant person, resource, or process—without revealing confidential information.

Compliance Graph, Ethics Automation, and Proof-of-Trust Attestations

The Compliance Graph serves as a machine-readable rule engine mapping legal, fiduciary, and professional-ethics policies into executable logic. It continuously monitors participants and entities, recording outcomes as immutable audit events and automatically suspending, reclassifying, or dissolving rights when violations occur. All compliance events generate cryptographically verifiable proofs that can be disclosed to regulators or auditors without revealing underlying identities.

Proof-of-Trust Enforcement Flow and Machine-Enforced Law

The Proof-of-Trust (PoT) layer ensures that every operation — including data access, consent verification, and value exchange — is executed under valid, auditable authority.

Core components include:

- **Trust Credential:** A cryptographically signed token proving lawful authority to act.
- **Trust Block:** An immutable record of a verified consent, delegation, or transaction.
- **Trust Policy Graph:** A distributed rule graph defining permissible relationships between entities and jurisdictions.
- **PoT Verifier:** An AI-assisted validator confirming compliance and consent before execution.

Each event produces a **Trust Block** cryptographically linked to prior lineage, providing tamper-proof, privacy-preserving auditability for regulators or authorized verifiers.

Machine-Enforced Law.

The Proof-of-Trust (PoT) layer operationalizes statutory and contractual obligations as executable code. Every event—whether data access, contracting, or payment—executes only when a valid, cryptographically verifiable Trust Credential exists. This converts compliance and ethics requirements from manual, post-hoc review into automatic, pre-execution enforcement, establishing the world's first *machine-enforced law* for privacy, fiduciary duty, and accountability.

Policy-Driven Redistribution and Public-Benefit Alignment

When participation rights cannot lawfully activate, the system automatically reallocates restricted value toward **Public-Benefit Derivative Rights (PBDR)** pools or compliant substitutes. Each PBDR pool routes value to authorized social, research, educational, healthcare, environmental, or other public-benefit programs under verifiable provenance. All redistributions are recorded as encrypted, tamper-evident audit proofs preserving

lawful continuity. Alternatively, the system may dynamically substitute compliant participants or providers so that intended functions proceed without interruption or disclosure.

Privacy-Preserving Governance and Auditability

Operational data resides within privacy-preserving domains enforcing encryption, access control, and policy-based disclosure. Governance actions—including creation, activation, suspension, or redistribution—are encoded as **Trust Blocks** or equivalent attestations containing only minimal necessary information. This architecture enables verifiable compliance while maintaining lawful secrecy and protecting participants from coercion, reputational risk, or unauthorized exposure.

Population-Scale Automation and Continuity

The system supports zero-marginal-cost creation, monitoring, and maintenance of thousands to millions of Quantum Privacy Cells. Automated orchestration routines manage lifecycle events, reconstituting or merging compartments upon policy or regulatory change, changes in employment status, conflicts, or fiduciary duties, or other factors that influence legal, policy, or ethical compliance, all while preserving provenance and ring-fenced liability. Dormant entities may be reactivated when conditions are satisfied, ensuring continuous, adaptive compliance across evolving frameworks.

3.2 Integration with Identity and Consent Frameworks

Building on the substrate above, the invention integrates natively with identity and consent services to enable frictionless, lawful onboarding. Through **EasyAccess** and **Personal Privacy Network (PPN)** services, individual opt-in automatically authorizes creation of a corresponding Quantum Privacy Cell or Series.

- The EasyAccess Consent API or embedded Terms-of-Service clause serves as lawful authorization.
- The resulting **Personal QPNs (Quantum Privacy Cells)** provide limited-liability participation, enabling lawful engagement and rewards without personal exposure.
- Rights remain dormant until compliance verification completes, at which point activation occurs automatically.
- Participants may deactivate their QPNs, suspending activity while preserving encrypted audit integrity for provenance and benefit allocation.

This integration allows viral, privacy-preserving onboarding of millions of participants while maintaining verified compliance and ethical safeguards.

In a preferred embodiment, the invention operates through **Quantum Privacy LLC**, a Delaware Series Limited Liability Company governed by multiple Managers under an

Executive Director acting ex officio. The entity functions within the **Quantum Privacy Exchange (QPX)** ecosystem to automate Quantum Privacy Cell formation, compliance verification, and lawful value distribution.

3.3 Automatic Quantum Privacy Cell Creation and EasyAccess Enrollment

When an individual or organization opts into an EasyAccess service or activates a PPN, the system automatically creates a corresponding Quantum Privacy LLC Series ("Quantum Privacy Cell", or "QPC") on behalf of that participant. This QPC acts as a private, limited-liability Quantum Privacy Cell representing that participant's verified identity, rights, and benefits within the Quantum Privacy Ecosystem. Digital consent—recorded through the EasyAccess Consent API or embedded within a participating organization's Terms of Service or Privacy Policy—serves as lawful authorization for Series creation. No additional signature or contract review is required: cryptographically signed consent records and Proof-of-Trust attestations provide full legal evidence of authorization under electronic-signature and consent laws.

EasyAccess Authorization (Required Elements — Reference Language)

"By opting in to EasyAccess (or other brand), you authorize a Personal Privacy Network to use encrypted and anonymized information to verify identities and conveniently authorize access to apps, data, secure messages, accounts, digital content, and online services.

Your Personal Privacy Network will not disclose personally identifiable information to any person or system without your explicit permission and will protect you with:

- End-to-end encryption of your data, interactions, and messages across different apps, devices, browsers, and messaging clients;
- Independent verification of the people, organizations, and systems you interact with;
- Personal control over your privacy, consent, and data-access policies;
- Anonymous authorization, enabling you to verify credentials or access services without revealing your identity or sensitive personal information; and
- Optional EasyAccess Rewards that share a portion of the value created through your Privacy Network participation, all protected by Quantum Privacy™."

This reference consent text exemplifies how a single privacy-preserving API call or online acknowledgment can serve as both legal consent and technical trigger for Quantum Privacy Cell instantiation, ensuring frictionless, compliant onboarding at population scale.

3.4 Quantum Privacy Cell Registration, Binding, and Private Governance

Upon acceptance, the system automatically instantiates the participant's QPC, records encrypted metadata (purpose, rights, jurisdiction, and Trust Block linkage), and binds the record to the participant's PPN. Each QPC operates under confidentiality; participants incur no personal liability and maintain full control over their PPN credentials. All books, records, and agreements remain encrypted within the participant's privacy domain and are auditable only through policy-authorized Proof-of-Trust requests.

Quantum Privacy Cell Recognition Terms (Reference Language)

A Quantum Privacy Cell (QPC) is a private, limited-liability structure created by Quantum Privacy LLC to recognize your participation and protect your privacy.

- You incur no personal obligations or liabilities by being a QPC Beneficiary.
- Your QPC operates confidentially and exists solely to help you manage your verified identity, rights, and benefits within the Quantum Privacy™ and Quantum Privacy Exchange ecosystem.
- Your QPC provides a secure way to receive EasyAccess Rewards and other verified value earned through your lawful engagement or consented participation—while maintaining full privacy and compliance with applicable laws and ethical standards.
- All records are encrypted and maintained privately within your Personal Privacy Network, accessible only under your control.
- Your QPC allows you to contract, interact, and receive benefits anonymously, using privacy-preserving credentials instead of revealing personally identifiable information.
- You may deactivate your QPC, which will suspend active participation and restrict all access to associated data while preserving the integrity of encrypted audit records for lawful provenance and benefit allocation.

These statements are illustrative, not limiting; they demonstrate how participant-facing notices can explain the benefits and protections inherent in a manager-originated Quantum Privacy Cell.

3.5 Lawful Activation, Verification & PPN Integration of Quantum Privacy Cells

All rights, privileges, and benefits associated with a **Quantum Privacy Cell (QPC)** remain dormant until verified under the **Unified Trust Model (UTM)** and **Proof-of-Trust (PoT)** frameworks. These mechanisms ensure that activation occurs only after confirming compliance with all applicable fiduciary, employment, conflict-of-interest, anti-bribery, and ethical requirements. No token issuance, value realization, or contractual execution proceeds until these validations are complete.

If eligibility fails or subsequently expires, the affected rights are automatically converted into **Restricted Derivative Rights (RDR)** and redirected to authorized **Public-Benefit**

Derivative Rights (PBDR) pools, or substituted with compliant participants—preserving lawful continuity while preventing unlawful inducement or unjust enrichment.

Each QPC maintains encrypted provenance records within its associated **Personal Privacy Network (PPN)**, enabling verifiable audits and compliance attestations without revealing personal or proprietary data. All verification and audit operations are conducted through privacy-preserving proofs that ensure complete confidentiality while maintaining full traceability and accountability. Participants may voluntarily deactivate their QPC or Series at any time, suspending participation yet retaining immutable audit records for provenance, attribution, and lawful benefit tracking.

Enterprises, institutions, and service providers that embed the **EasyAccess Consent API** can automatically instantiate compliant Quantum Privacy Cells for their employees, customers, partners, or online users. This mechanism supports population-scale, privacy-preserving onboarding and continuous compliance enforcement across diverse sectors—including healthcare, finance, education, sustainability, and public governance. Through these integrations, **Quantum Privacy LLC** and its QPC-based governance architecture serve as a universal, lawful gateway for distributed participation, enabling secure collaboration, resource sharing, and benefit realization across the **Quantum Privacy Exchange (QPX)** ecosystem.

3.6 Alternative Jurisdictional and Technical Embodiments

While the **Delaware Series LLC** framework represents a preferred embodiment, equivalent legal and technical structures may be applied globally to achieve the same functional results. Each embodiment enables confidential entity formation, deferred activation, and policy-driven redistribution of rights under the **Unified Trust Model (UTM)** and **Proof-of-Trust (PoT)** verification framework, while conforming to the legal, tax, and fiduciary requirements of its jurisdiction.

Alternative Legal and Jurisdictional Frameworks

Comparable implementations may utilize any of the following entity types or governance constructs:

- **U.S. Entities:** Delaware, Nevada, or Wyoming Series LLCs; C-Corporations; or trust-structured vehicles.
- **International Entities:** Cayman Islands Segregated Portfolio Companies (SPCs); British Virgin Islands companies; Abu Dhabi Global Market (ADGM) or Dubai International Financial Centre (DIFC) private companies; and **Incorporated Cell Companies (ICCs)** or **Protected Cell Companies (PCCs)** in Jersey, Guernsey, Malta, Gibraltar, the Isle of Man, or Mauritius.

- **Tokenization and Custody Frameworks:** Licensed custodians or regulated token-service providers managing digital or derivative rights under compliance supervision.

Each structure maintains **functional equivalence**—confidential governance compartmentalization, deferred activation, and policy-driven redistribution—while adapting to the enforceability and regulatory standards of its host jurisdiction.

Alternative Technical and Computational Substrates

The same invention may be implemented on diverse technical infrastructures, including:

- **Distributed-Ledger Systems:** Hedera Hashgraph, Hyperledger Fabric, Ethereum, or other directed-acyclic-graph (DAG) or blockchain variants supporting privacy-controlled records.
- **Cryptographic Privacy Techniques:** Zero-knowledge proofs (zk-SNARKs, zk-STARKs), secure multi-party computation (SMPC), and homomorphic encryption.
- **Confidential-Computing Environments:** Trusted execution enclaves such as Intel SGX, AMD SEV, AWS Nitro, or Microsoft Entra providing verifiable isolation and attestation.
- **Compliance-Automation Engines:** Policy-orchestration frameworks and rule engines that translate jurisdiction-specific laws and ethics codes into machine-verifiable constraints.

All such variants interoperate under the **Unified Trust Model (UTM)**, ensuring seamless cross-jurisdictional reuse, verifiable compliance, and lawful interoperability across heterogeneous infrastructures.

The **Quantum Privacy Exchange (QPX)** and **Quantum Privacy Accelerators (QPAs)** may incorporate **Quantum Privacy Cells (QPCs)** instantiated across multiple jurisdictions, entity types, and technical substrates, provided that their governing legal instruments and operational policies remain harmonized under the **Unified Trust Model (UTM)**. When participating QPCs demonstrate equivalent **Proof-of-Trust (PoT)** attestations and adhere to federated policy-enforcement and governance standards, they function as interoperable components of a single lawful ecosystem—preserving compliance, provenance, and verifiable trust across organizational and jurisdictional boundaries.

3.7 Legal and Ethical Compliance Framework

The invention embeds legal and ethical constraints directly into activation and governance mechanisms. Deferred activation ensures no right or benefit can serve as an inducement or improper advantage before verified authorization. The Compliance Graph continuously

monitors obligations, suspending or dissolving rights upon detection of conflict or breach. All disclosures are policy-constrained and exportable as verifiable proofs to auditors or regulators without exposing confidential participants. This framework aligns with international standards, including but not limited to SEC fiduciary guidance, the OECD Anti-Bribery Convention, and G-20 corporate-governance principles, providing cross-jurisdictional interoperability.

3.8 Regulatory and Legal Enablement & Automated Enforcement of Data Rights

The Unified Trust Model (UTM) and Proof-of-Trust (PoT) frameworks together provide a regulator-grade foundation for lawful participation, disclosure control, and automated enforcement of individual, institutional, and governmental rights across all embodiments of the invention. In practical terms:

1. **Eligibility, conflicts, and ethics** are verified before any right or benefit activates.
2. **Privacy-preserving proofs** are exportable to regulators or auditors without revealing identities or trade secrets.
3. **Rights that cannot lawfully vest** are automatically reclassified as *Restricted Derivative Rights (RDRs)* and rerouted to *Public-Benefit Derivative Rights (PBDR)* pools with full cryptographic provenance.

Collectively, these mechanisms operationalize statutory data-access and participation frameworks under **GDPR (Arts. 15–20)**, **CCPA/CPRA (§§ 1798.100–1798.125)**, **HIPAA Privacy Rule § 164.524**, **FERPA § 99.10**, **IRS Code § 6103**, and equivalent laws governing lawful access, audit, and correction of data across jurisdictions.

Under the **Delegation-of-Rights Architecture**, a person's **Personal Privacy Network (PPN)** and its paired **Quantum Privacy Cell (QPC)** act jointly to assert or delegate the individual's legal, regulatory, and contractual rights in every sphere of life—whether as a consumer, employee, citizen, taxpayer, patient, parent, student, or entrepreneur. Acting as the individual's operational privacy agent, the PPN verifies identity, consent, and lawful authorization, while the QPC provides the limited-liability governance compartment that enforces those rights, allocates benefits, and ensures compliance.

Together they enable the direct, privacy-preserving invocation and lawful exercise of **access, correction, use, and participation rights** arising under any recognized **legal, regulatory, contractual, or policy authority**, including:

- **Statutory and Regulatory Rights** — Rights defined in thousands of federal, state, local, and international statutes, regulations, and ordinances governing access, disclosure, portability, and correction of personal or institutional data.

- **Contractual Rights** — Rights established through service agreements, employment or participation contracts, nondisclosure agreements, and digital-service terms that control or authorize lawful data use or system access.
- **Corporate Policies and Fiduciary Duties** — Rights or permissions derived from corporate bylaws, fiduciary obligations, ethics frameworks, and compliance rules adopted by enterprises or institutions.
- **Licensing, Intellectual-Property, and Content Rights** — Rights arising from data-sharing agreements, software and content licenses, open-data terms, or creative and research collaborations.
- **Delegated and Agency-Based Rights** — Powers exercised through lawful representation, including agency relationships, guardianships, trusteeships, powers of attorney, or employer-employee delegations.
- **Public-Sector and Civic Access Rights** — Rights to obtain, review, and control government-held information under freedom-of-information, public-records, administrative-procedure, and due-process provisions.
- **Ethical and Consent-Based Rights** — Rights rooted in informed-consent protocols, professional codes, and research-ethics standards that govern lawful collection and use of personal or proprietary data.

These legal, contractual, and policy foundations collectively encompass and operationalize the broad spectrum of sector-specific statutory frameworks, including:

- **Healthcare, Education & Social Services:** *HIPAA* (45 C.F.R. § 164.524 et seq.), *42 C.F.R. Part 2* (substance-use records), *FERPA* (20 U.S.C. § 1232g), *SOPIPA* (Cal. Bus. & Prof. Code § 22584 et seq.), and the *Privacy Act of 1974* (5 U.S.C. § 552a).
- **Financial, Tax & Credit:** *IRS § 6103*, *FCRA/FACTA* (15 U.S.C. § 1681 et seq.), *GLBA* (15 U.S.C. § 6801 et seq.).
- **Property, Court & Legal Records:** *FOIA* (5 U.S.C. § 552), state public-records laws, judicial-record-access rules, *PACER* (28 U.S.C. § 1913 note), and land-recording statutes.
- **Identity & Licensing:** *DPPA* (18 U.S.C. § 2721 et seq.) and analogous state driver-license privacy acts, vital-records, and licensing statutes.
- **Comprehensive Privacy Frameworks:** *GDPR*, *CCPA/CPRA*, *PIPEDA*, and state-level data-protection acts (e.g., VA CDPA, CO CPA, CT DPA, UT CPA).

The same architecture also accommodates **governmental and institutional authorities** to collect, process, and disclose information for legitimate public purposes—such as

taxation, benefits, law enforcement, education, public health, or emergency management—while ensuring that any resulting data exchange with a verified PPN or QPC occurs only under explicit consent, jurisdictional authority, and **Proof-of-Trust–verified compliance**.

By embedding these statutory, contractual, and policy frameworks directly into **UTM/PoT executable logic**, the invention converts compliance from a manual legal process into a **self-enforcing, machine-verifiable rule-of-law infrastructure**. It provides a unified and privacy-preserving mechanism for regulators, enterprises, and individuals to assert, fulfill, and audit lawful rights and obligations across jurisdictions—forming the operational foundation for **trusted digital governance and machine-enforced law**.

Inter-QPC Agreements

"Inter-QPC Agreements" refers to any legally binding agreement, memorandum of understanding, computational contract, or tokenized contractual arrangement executed among two or more **Quantum Privacy Cells (QPCs)**—each acting as the cryptographically sealed, limited-liability governance boundary for its respective participant under the Unified Trust Model (UTM).

Inter-QPC Agreements may govern collaborative participation in Quantum Privacy Accelerators, Exchange Networks, Resource Pools, or other coordinated activities; define revenue-sharing or derivative-rights allocations; establish shared Trust Criteria or Trust Credentials; or set interoperability and performance standards across jurisdictions, enterprises, or individuals.

Inter-QPC Agreements may be evaluated, verified, and enforced inside the EasyAccess Authorization Network or within the parties' Quantum Privacy Domains, enabling contractual conditions to be computed against proprietary, regulated, private, or personal data without revealing such data—or the identities of the contracting parties—to counterparties, intermediaries, or the network itself. This architecture enables robust, cross-organizational contractual enforcement among parties who may not know or trust each other, while maintaining strict compliance with privacy, cybersecurity, confidentiality, and regulatory requirements.

All Inter-QPC Agreements are embodied as legal contracts, executable smart contracts, or computable Trust Blocks recorded within the Privacy Network Exchange and enforced through Proof-of-Trust (PoT) verification. They are automatically subject to the confidentiality, indemnification, attribution, and compliance provisions of the Unified Trust Model and the Quantum Privacy Cell Participation Agreement, enabling globally scalable, privacy-preserving contractual coordination.

Operational Scenarios

Operational scenarios supported by this framework include:

1. ***PPN-Asserted Access***: A QPC, acting through PoT credentials, issues a standardized, verifiable rights-request (e.g., HIPAA access, FERPA transcript, FOIA petition). The custodial agency validates the claim under the UTM and returns encrypted records directly to the requester's PPN.
2. ***Enterprise/Government-Initiated Sharing***: Agencies or enterprises voluntarily transmit verified personal or public-benefit data to PPNs as a service or statutory obligation (e.g., benefits eligibility, age verification). Such transfers may be logged as *Resource Contributions* eligible for fractional Exchange-Token credit.
3. ***Hybrid Cooperative Exchange***: An agency notifies a person's PPN of relevant records and provides instructions for asserting rights; after successful retrieval, value allocations are divided among the beneficiary, Exchange Providers, and Trust Authorities that verified the exchange.

By embedding these statutory rights and obligations directly into executable **UTM/PoT logic**, the Quantum Privacy framework transforms compliance from a manual legal process into a **self-enforcing, machine-verifiable rule-of-law substrate**. It provides regulators, enterprises, and citizens with a unified, privacy-preserving mechanism for asserting and fulfilling lawful data-access and participation rights across all sectors, jurisdictions, and infrastructures — forming the technical foundation for **machine-enforced law** and equitable digital governance.

Employment, Fiduciary & Professional-Compliance Constraints

A wide range of regulated professionals—including corporate executives, employees, fiduciaries, attorneys, auditors, investment bankers, asset managers, physicians, researchers, and public officials—operate under overlapping legal, contractual, and ethical restrictions that tightly govern how they may engage in external economic or governance systems. Employment agreements often include invention-assignment clauses, non-competition covenants, non-solicitation restrictions, and strict conflict-of-interest policies. Professionals in advisory or fiduciary roles are further bound by client-confidentiality requirements, insider-information rules, securities-law duties, and standards of professional conduct imposed by governing bodies such as the SEC, FINRA, PCAOB, ABA, AICPA, and state licensing authorities.

Under these regimes, even the *appearance* of contingent compensation, undisclosed value rights, token allocations, or governance influence can constitute a prohibited inducement or conflict. Public or semi-public systems—including traditional blockchains, DAO governance models, or transparent token ledgers—therefore expose regulated

participants to the risk of breaching employment contracts, violating fiduciary obligations, or triggering professional-ethics sanctions. Merely being *discoverable* as holding a contingent economic interest can violate anti-bribery laws such as the U.S. Foreign Corrupt Practices Act (FCPA), 18 U.S.C. § 201, the OECD Anti-Bribery Convention, and the U.K. Bribery Act.

The Unified Trust Model (UTM) and Proof-of-Trust (PoT) frameworks resolve these compliance barriers by ensuring that all participation rights—equity-like interests, compensation rights, governance privileges, and derivative allocations—remain cryptographically dormant and undiscoverable until eligibility is verified. Through encoded Trust Criteria and the Compliance Graph, the system automatically enforces employment restrictions, fiduciary rules, and jurisdiction-specific ethics standards before activating any right or benefit. Where eligibility is not satisfied, the system ensures lawful continuity by substituting a verified compliant actor or routing the unvested value into Public-Benefit Derivative Rights (PBDR) pools with full cryptographic provenance.

By embedding employment, fiduciary, professional-conduct, and regulatory constraints directly into the trust-verification substrate, the QPX transforms compliance from a manual legal obligation into a self-executing property of the infrastructure. Regulated professionals may lawfully participate, contribute, and receive proportional recognition—without breaching contractual duties, exposing confidential affiliations, or risking prohibited inducements.

Anti-Bribery, Inducement, and Ethics-Regime Enforcement

Participants operating in regulated or public-interest roles are subject to stringent anti-bribery and conflict-of-interest laws that strictly limit how value, recognition, or contingent benefits may be offered, accepted, or even implied. Statutes such as the U.S. Foreign Corrupt Practices Act (FCPA), 18 U.S.C. § 201 (public-sector bribery), the U.K. Bribery Act 2010, the OECD Anti-Bribery Convention, and equivalent laws in the EU, Middle East, and Asia impose liability not only for actual bribery, but for **any appearance of undue influence, contingent benefit, or undisclosed relationship**.

Traditional blockchain, DAO, and token-governance systems inherently expose participants' affiliations, contingent rights, and financial interests through publicly accessible ledgers, mempool activity, governance votes, or staking records. For regulated professionals—including corporate executives, fiduciaries, government staff, procurement personnel, academic researchers, and public officials—simple *discoverability* of potential upside, token allocation, or governance influence may constitute an unlawful inducement or prohibited conflict. Because these systems cannot condition, conceal, or defer the recognition of interest until ethical and statutory prerequisites are met, they remain fundamentally incompatible with established anti-bribery and ethics regimes.

The Unified Trust Model (UTM) and Proof-of-Trust (PoT) frameworks resolve these conflicts by ensuring that all participation rights, derivative allocations, governance privileges, and revenue-linked benefits remain cryptographically dormant, undiscoverable, and non-realized until all applicable anti-bribery, procurement-ethics, and conflict-of-interest rules are verified. Eligibility is evaluated using encoded Trust Criteria and Compliance Graph logic that incorporate statutory prohibitions, organizational codes of conduct, procurement protocols, and jurisdiction-specific ethics rules.

If a conflict, disallowed inducement, or statutory disqualification is detected, the system automatically executes a lawful resolution pathway. This includes (i) confidential substitution of a verified compliant actor, (ii) rerouting of unvested benefits to Public-Benefit Derivative Rights (PBDR) pools, or (iii) cryptographically preserving rights as Restricted Derivative Rights (RDRs) pending re-evaluation. All actions maintain provenance through privacy-preserving Trust Blocks, enabling auditable regulatory assurance without exposing private identities or sensitive relationships.

By embedding anti-bribery and ethics-compliance enforcement directly into the cryptographic substrate, the QPX transforms legal and ethical constraints into continuous, machine-verified guardrails. This ensures that regulated professionals, public officials, and institutional actors may participate in collaborative, tokenized ecosystems without violating procurement rules, ethics standards, or national and international anti-corruption laws.

3.9 Controller / Processor and Delegated-Authority Equivalency

Under prevailing privacy, data-protection, and fiduciary law, the **Personal Privacy Network (PPN)** operates as the **individual's authorized agent**, not as an independent controller or processor. The paired **Quantum Privacy Cell (QPC)** functions as the individual's **limited-liability governance compartment**, enforcing accountability, provenance, and benefit allocation under the Unified Trust Model (UTM).

This configuration preserves the **individual as the ultimate data controller** within the meaning of **GDPR Art. 4(7)** and **CCPA § 1798.140(v)**, while enabling lawful delegation of operational, contractual, and fiduciary functions to the PPN and QPC. Because the individual retains lawful control and all processing occurs within privacy-preserving compartments acting under delegated authority, the system **eliminates the need for separate enterprise-to-enterprise data-sharing or processing agreements**, enabling compliant, privacy-preserving interoperability across enterprises, sectors, and jurisdictions.

Beyond data-access regulation, this framework extends to **all lawful rights and obligations that can be delegated, asserted, or fulfilled by an agent** under statutory,

contractual, fiduciary, or policy authority. These include—but are not limited to—rights of identity verification, consent management, contract execution, financial or fiduciary authorization, intellectual-property licensing, and cross-jurisdictional policy enforcement.

The **Delegation-of-Rights Architecture** disclosed herein thus provides full legal and technical enablement for:

- **Delegated authority chains** and agentic representation across personal, corporate, and governmental domains;
- **Proof-of-Trust enforcement** ensuring each action and transaction is verified, lawful, and non-repudiable; and
- **Rights assertion, fulfillment, and provenance tracking** under any lawful basis—statutory, regulatory, contractual, or ethical—within and across the Quantum Privacy Exchange (QPX).

By aligning data-protection doctrine with agency law, fiduciary governance, and cryptographic proof mechanisms, the PPN/QPC framework establishes a globally interoperable model for **lawful, automated rights execution and accountability**—redefining the boundaries between data subject, data controller, and data processor in a privacy-preserving, self-governing ecosystem.

3.10 Tokenization and Exchange Integration

In certain embodiments, the invention interoperates with tokenized participation systems—including, but not limited to, the **Quantum Privacy Token (QPT)** classes (also referred to as PNX Tokens)—which together form the foundation of the **Quantum Privacy Exchange (QPX)** economy. These token classes represent trust-verified rights, obligations, and value flows across distributed ecosystems governed by the **Unified Trust Model (UTM)** and **Proof-of-Trust (PoT)** accreditation frameworks.

Core Token Classes

- **Exchange Tokens (EXCH)** – Trust-verified settlement instruments representing rights to value generated through lawful collaboration, verified resource use, and recombination events. EXCH Tokens serve as attribution and settlement units—earned through verifiable participation and Proof-of-Trust validation, not speculative purchase—ensuring they operate as **utility-based performance tokens**, not investment contracts.

  (See October 2025 Provisional §§ 3.3–4.2, Figs. 3–4.)

- **Resource Tokens (RT)** – Asset-backed, privacy-preserving digital representations of data, compute, AI models, intellectual-property rights, legal contracts, or any other resources or assets. RTs establish provenance, valuation, and authorized use

conditions for each resource, forming the **atomic unit of tokenized exchange** within the QPX ecosystem. Each RT carries embedded policy metadata defining lawful purpose, consent, jurisdiction, and reuse constraints, recorded as Trust Blocks under UTM.

- **Resource Pool Tokens (RPT)** – Aggregated liquidity and pooling vehicles representing pro rata interests in collections of Resource Tokens or their derivatives. RPTs enable efficient syndication, reuse, and liquidity creation across sectors, providing institutional-grade mechanisms for shared ownership and collective yield generation consistent with privacy-preserving compliance frameworks.

  (See October 2025 Provisional § 5.1.)

- **Accelerator Tokens (AT)** – Programmatic attribution and reward instruments issued by **Quantum Privacy Accelerators (QPAs)** to participants contributing verified value, governance, technical resources, or—in combination with conventional financing instruments such as SAFE Notes, convertible debt, or equity issued by Accelerator-affiliated entities—investment capital.

  ATs serve as **lawful participation and allocation tokens**, enabling attribution, referral, and reward sharing among innovators, investors, and ecosystem builders without constituting securities. They are not purchased for consideration; instead, they are **earned or allocated** following verified participation or capital infusion via compliant financing vehicles, separating the **investment instrument (SAFE or equity)** from the **participation token (AT)**. This model mirrors the compliance logic detailed in the October 2025 Provisional (§§ 4.1–5.4) and the November Provisional § 4 (*Quantum Privacy Accelerator Systems and Methods for Self-Funding, Trust-Verified Market Formation*), ensuring regulatory conformity and cross-sector interoperability.

- **EasyAccess Reward Tokens (EART)** – Consent-linked engagement instruments that reward verified outreach, advocacy, and user activation through **EasyAccess links**, **EasyAccess Consent–enabled applications**, or **Quantum Privacy–compliant digital content**. EARTs serve as lawful onboarding and adoption incentives, allowing individuals to earn verified recognition for promoting, sharing, or participating in trusted interactions. They function as a privacy-preserving bridge between everyday user engagement and the formal Quantum Privacy Token economy, ensuring that all incentives and value transfers remain compliant under the Unified Trust Model (UTM) and Proof-of-Trust (PoT) verification frameworks, ensuring that each engagement remains privacy-preserving, non-inducive, and compliant with applicable jurisdictional and ethical standards.

- **Privacy Network Tokens (PNT)** – Hybrid governance and participation rights associated with contributions within **Quantum Privacy Networks (QPNs)** or **Enterprise Privacy Networks (EPNs)**. PNTs act as verifiable identity and provenance anchors, binding lawful consent, reputation, and participation history under UTM, thereby supporting decentralized yet accountable governance.
- **Exchange Root Tokens (ERT)** – Universal network-level participation tokens representing fractional rights to all Exchange Tokens generated across the QPX ecosystem.

  ERTs aggregate verified value across all Accelerators, Exchanges, and Resource Pools and are treated as **capital-asset-class property rights**, not securities, under global accounting and tax frameworks.

Architecture and Interoperability

Each Quantum Privacy Accelerator (QPA) acts as an issuance and governance domain for its respective token classes.

Token issuance, routing, and settlement events are recorded as verifiable **Trust Blocks** under UTM and anchored through the **PoT Consensus Service** (e.g., Hedera HCS or equivalent hybrid-ledger frameworks).

This structure supports **Trust-Weighted Liquidity Pools** and cross-domain token exchange, enabling fiat on/off-ramps, multi-jurisdictional compliance, and privacy-preserving financial interoperability.

Governance and Compliance Integration

All token events—including minting, allocation, redistribution, and redemption—operate under continuous UTM/PoT verification. Embedded policy logic enforces jurisdictional, fiduciary, and ethical constraints directly within token metadata, transforming compliance into a **machine-enforced property of every transaction**.

Issuance entities may include Delaware Series LLCs, Cayman SPCs, ADGM/DIFC private companies, or regulated custodians—each verified under Proof-of-Trust attestation and harmonized through the Unified Trust Model.

Optional **token-based securitization or ETF-style aggregation** may be employed to facilitate institutional liquidity while preserving baseline treatment as **capital assets or property rights**, not securities. This approach ensures lawful global participation while maintaining functional parity with traditional fiduciary and accounting standards.

Functional Role within the Quantum Privacy Exchange

Within QPX, these token classes provide the connective tissue linking privacy-preserving governance, lawful economic participation, and decentralized value realization. They

translate verified contributions, rights, and trust credentials into composable, auditable, and interoperable digital assets—supporting lawful, self-funding collaboration across sectors, jurisdictions, and infrastructures.

Tokenization remains optional: all compliance, governance, and value-tracking functions are enforceable through legal artifacts, verified records, and Trust Blocks alone. When implemented, however, the token layer enables scalable interoperability, real-time liquidity, and transparent value attribution across the global Quantum Privacy ecosystem.

Cross-References:

See § 2.9 (*Quantum Accelerator Architecture for Decentralized Innovation*) for incentive and liquidity mechanics;

§ 3.8 (*Regulatory and Legal Enablement under the Unified Trust Model and Proof-of-Trust*) for embedded compliance logic;

and § 4 (*Quantum Privacy Accelerator Systems and Methods for Self-Funding, Trust-Verified Market Formation*) for lawful fundraising, redistribution, and market-layer integration.

4. Quantum Privacy Exchange Participation & Universal Adoption Model

The preceding section established the legal and technical architecture of Quantum Privacy Cells and their governance under the Unified Trust Model and Proof-of-Trust verification. Section 4 now turns to how those mechanisms operate in practice—connecting people, enterprises, and institutions into a living ecosystem.

The Quantum Privacy Exchange (QPX) transforms these foundational elements into a participatory framework for lawful collaboration, self-funding growth, and viral adoption across sectors and jurisdictions. To support these interactions, exchange-level coordination, commercial terms, and joint-use rights may be established through Inter-QPC Agreements (see § 3.8), ensuring privacy-preserving contractual governance across participants.

4.1 Structural Inefficiencies of Venture, Private Equity, & Traditional Innovation Systems

Conventional venture-capital, private-equity, corporate-innovation, and government-funding systems suffer from deep structural limitations that prevent broad-based, equitable, or efficient innovation – particularly for global-scale core infrastructure.

These legacy models depend on centralized decision-making, sequential fundraising cycles, opaque governance structures, and rigid participation pathways that restrict

access to a narrow subset of wealthy investors, well-connected insiders, or privileged institutions. As a result, innovation capacity is artificially throttled by capital concentration rather than expanded by global participation.

These systems impose exceptionally high costs of capital—frequently exceeding 25–40% when accounting for management fees, performance fees, and dilution—while simultaneously restricting participation to those already possessing significant financial, political, or institutional leverage. Governance dynamics are dominated by consensus-seeking committees, herd-based investment patterns, and short time horizons that prioritize "hot sectors" over long-term, foundational innovation. This system amplifies inequality by limiting meaningful ownership or value realization to a small circle of actors, excluding the vast majority of contributors, domain experts, and end users who actually create or validate real-world impact.

The structural inefficiencies extend beyond capital flows. Because ownership, compliance, and data rights are siloed within individual organizations, traditional models cannot lawfully pool regulated, proprietary, or personal resources such as data, intellectual property, compute infrastructure, or specialized human expertise. Cross-organizational collaboration requires costly bilateral contracting, manual compliance verification, and slow due-diligence processes. These frictions suppress reuse of resources, constrain the pace of innovation, and prevent solutions from forming dynamically across institutions, markets, and jurisdictions.

As a consequence, trillions of dollars in latent human, digital, financial, and ecological capacity remain trapped in disconnected organizational silos. Innovation cycles grow slower, riskier, and less equitable, while global challenges in health, sustainability, education, security, and public infrastructure continue to outpace the ability of legacy capital systems to respond.

The Quantum Privacy Accelerator (QPA) and Quantum Privacy Exchange (QPX) architectures directly address these systemic failures by embedding liquidity, compliance, trust-verified participation, and dynamic, cross-organizational resource orchestration into the fabric of collaboration itself. By enabling any lawful participant—individual, enterprise, or government—to contribute resources through Quantum Privacy Cells (QPCs) under deferred activation, verifiable compliance, and privacy-preserving provenance, the QPX transforms the economics of innovation from exclusive, centrally mediated capital allocation into a self-funding, continuously liquid, and globally inclusive ecosystem.

In this model, resource contributions, solution formation, network expansion, and public-benefit alignment become intrinsic drivers of value creation rather than incidental by-products. Markets form organically through Inter-QPC Agreements, Resource Pools, and Exchange Networks that align incentives, reduce friction, and enable lawful reuse of high-

value assets across jurisdictions. The result is a paradigm shift: innovation becomes participatory at population scale, liquidity becomes continuous and compliance-verified, and value is allocated proportionally to verified contribution rather than access to capital or institutional privilege.

Section 4.2 and the subsections that follow describe how Quantum Privacy Accelerators operationalize this transformation, enabling efficient, lawful, and self-optimizing market formation across all domains of economic and social activity.

4.2 Trust-Verified Capital Formation for Accelerators

The Quantum Privacy Accelerator (QPA) model enables lawful, self-funding participation and capital formation without triggering investment-security classification. Funding occurs through conventional, regulator-recognized instruments—such as **SAFE Notes**, **convertible notes**, **equity issuances**, or **debt obligations**—executed by the Accelerator's legal entity (e.g., Delaware Series LLC, Cayman SPC, or ADGM/DIFC company). These instruments establish the investor's legal relationship with the entity, while **Accelerator Tokens (ATs)** operate in parallel as *non-speculative attribution and reward mechanisms* distributed after verified participation or activation.

Capital Formation and Verification

Each QPA may raise working capital or seed funding through its associated legal entity under standard corporate law. Upon capital acceptance, Proof-of-Trust (PoT) verification records the lawful source, jurisdiction, and compliance status of all contributions. Once verified, ATs or other participation tokens may be allocated to investors, founders, or referrers as a proportional recognition of verified value creation—not as consideration for investment itself. This separation of *financial instrument* and *participation token* preserves compliance under the Howey, Reves, and FinHub frameworks, preventing token treatment as a security.

Referral- and Participation-Based Rewards

Accelerators may allocate limited AT pools to reward verified referrals, ecosystem advocacy, or resource contributions that increase lawful participation. Such allocations are triggered through EasyAccess Consent or authenticated Proof-of-Trust attestations, ensuring that referral rewards qualify as *earned compensation or promotional consideration*, not investment returns. All allocations are logged as Trust Blocks under the Unified Trust Model, creating permanent auditability and regulatory transparency.

Automated Redistribution and Conflict Mitigation

When a participant's rights remain unactivated or restricted due to fiduciary or ethical constraints, those allocations convert automatically into **Restricted Derivative Rights (RDRs)** and are rerouted into **Public-Benefit Derivative Rights (PBDR)** pools, ensuring

lawful redistribution to compliant beneficiaries or public-interest initiatives. These self-executing reallocation rules are enforced under PoT policy logic and verified through independent Trust Authorities, maintaining continuous ethical alignment across all fundraising and participation events.

Compliance and Cross-References

All fundraising, allocation, and redistribution actions are governed by the Unified Trust Model (UTM) and recorded as privacy-preserving Trust Blocks. This structure converts capital-formation compliance into a *machine-enforced property* of the network itself—eliminating manual reporting risk and enabling global regulatory interoperability.

See also:

- § 2.9 (*Quantum Accelerator Architecture for Decentralized Innovation*) — self-funding incentive design;
- § 3.8 (*Regulatory and Legal Enablement under the Unified Trust Model and Proof-of-Trust*) — compliance logic

4.3 Key Advantages and Operational Outcomes

Collectively, the Quantum Privacy Exchange (QPX), Quantum Privacy Accelerators (QPAs), and associated governance frameworks deliver a unified, self-funding, and regulator-grade foundation for lawful digital collaboration and resource pooling. Together they enable privacy, trust, and compliance to function as intrinsic system properties rather than after-the-fact controls. Key advantages include:

- **Confidential and Lawful Participation** — Executives, consultants, public officials, researchers, and citizens can participate, collaborate, and receive verified recognition without breaching fiduciary, employment, or ethics restrictions.
- **Zero-Marginal-Cost Governance Automation** — Quantum Privacy Cells (QPCs) are created, verified, and maintained automatically under the Unified Trust Model (UTM), eliminating manual compliance and recordkeeping overhead.
- **Cryptographic Provenance and Auditability** — All actions, value transfers, and compliance events are recorded as verifiable Trust Blocks, ensuring immutable lineage and regulatory transparency without revealing private data.
- **Optional Tokenization and Self-Funding Rewards** — Quantum Privacy Tokens (QPTs) translate verified participation and lawful contributions into measurable value, sustaining ecosystem growth without external capital.
- **Population-Scale Onboarding and Verification** — EasyAccess Consent and Personal Privacy Networks (PPNs) provide seamless, privacy-preserving entry points for individuals and organizations worldwide.

- **Adaptive Compliance and Continuous Lawful Operation** — Dynamic substitution and policy-driven redistribution mechanisms maintain uninterrupted lawful continuity, even under changing participants, jurisdictions, or regulations.

4.4 Privacy-Preserving Compliance Service (PPCS)

The **Privacy-Preserving Compliance Service (PPCS)** constitutes a core subsystem of the UTM, providing continuous, automated verification of fiduciary, employment, contractual, and ethics requirements without exposing personally identifiable or commercially sensitive information. It transforms compliance from a static, manual review process into a real-time, privacy-preserving verification fabric that ensures lawful participation and traceable integrity across distributed ecosystems.

The Privacy-Preserving Compliance System (PPCS) integrates cryptographic identity proofs, jurisdictional policy graphs, and fiduciary rule templates to perform real-time conflict detection, affiliation screening, and rights classification. Each compliance evaluation executes within trusted-execution enclaves or equivalent privacy domains operating under homomorphic-encryption and zero-knowledge-proof protocols. Inputs may include employment status, fiduciary or board roles, contractual restrictions, regulatory registrations, or ethics filings obtained from verified registries or accredited **Trust Authorities**. Outputs consist solely of compliance attestations and classification directives—e.g., eligible, restricted, requires substitution, or redirect to PBDR—encoded as immutable Trust Blocks linked to the governing Quantum Privacy Cell.

When the PPCS detects a potential conflict or prohibited interest, the system automatically:

1. Reclassifies the affected allocation as a **Restricted Derivative Right (RDR)**;
2. Flags the associated Quantum Privacy Cell or Series for suspension, substitution, or adaptive remediation;
3. Routes the restricted value to a verified **Public-Benefit Derivative Right (PBDR)** pool or to a compliant substitute participant; and
4. Identifies alternative resources, participants, or process pathways that satisfy all applicable trust and compliance criteria—dynamically adapting workflow execution, contract routing, or benefit allocation to preserve lawful continuity without revealing confidential information.

All actions are cryptographically sealed and independently reviewable by authorized auditors or regulators, yet remain privacy-preserving and non-disclosive of underlying affiliations. These adaptive substitution mechanisms enable uninterrupted lawful operation even when a compliance constraint is encountered, ensuring that each process,

transaction, or collaboration proceeds with fully verified participants and auditable provenance.

The Privacy-Preserving Compliance System (PPCS) continuously synchronizes with jurisdictional policy feeds and enterprise ethics rules. When statutes, regulations, or employment conditions change, affected Quantum Privacy Cells automatically update their compliance state through the Compliance Graph, maintaining continuous lawful operation across organizations and jurisdictions.

Enterprises, government agencies, and professional associations may deploy localized instances of the PPCS within their **Enterprise Privacy Networks (EPNs)** to enforce internal compliance policies, perform due-diligence screening, or validate third-party participation. Because the PPCS exposes only verifiable proofs—not raw data—it enables cross-organizational compliance collaboration without breaching confidentiality, intellectual-property rights, or data-protection law.

The PPCS ensures that no value transfer, token issuance, or Quantum Privacy Cell activation occurs until all eligibility and ethics requirements are verified. It eliminates inducement, conflict-of-interest, and fiduciary-breach risk while preserving complete cryptographic auditability. Through its integration with the Proof-of-Trust framework, the PPCS forms the compliance backbone of the Quantum Privacy Exchange, supporting ethical, population-scale participation across jurisdictions and regulated sectors.

4.5 Financial Crime and Fraud Prevention Service (FCFPS)

Building upon the privacy-preserving verification principles of the PPCS, the **Financial Crime and Fraud Prevention Service (FCFPS)** extends the same logic to transactional integrity and anti-financial-crime enforcement within the PNX. The FCFPS provides continuous anti-money-laundering (AML), counter-terrorism-financing (CTF), sanctions-screening, and fraud-detection capabilities that operate natively within privacy domains. It aligns with global standards including but not limited to the U.S. Bank Secrecy Act (31 U.S.C. § 5311 et seq.), FinCEN guidelines, FATF Recommendations, and EU AMLD Directives.

Transactions and token transfers are analyzed using anonymized graph-analysis, zero-knowledge risk scoring, and other analytic methods. Instead of sharing personal data, nodes may exchange hashed identifiers and proof-of-lawful-source attestations. Suspicious patterns—such as rapid multi-jurisdictional transfers, circular flows, or credential anomalies—generate encrypted alerts verifiable by Trust Authorities without revealing participant identities.

Each Quantum Privacy Cell or wallet maintains a reputation ledger derived from verifiable compliance proofs and transaction behavior. Scores update dynamically based on positive

trust events (verified contributions, lawful redistributions) and negative indicators (failed verifications, sanctions hits). These anonymous reputations allow counterparties to evaluate trustworthiness without exchanging KYC data, preserving privacy while upholding financial integrity.

Accredited Trust Authorities—comprising regulated GRC vendors, enterprises, and governmental oversight bodies—may review FCFPS outputs through the **Proof-of-Trust Accelerator**. Each authority receives privacy-preserving compliance proofs sufficient to demonstrate regulatory conformity under its jurisdiction. Regulators can thus confirm lawful participation, AML/CTF diligence, and sanctions compliance without direct access to proprietary or personal information.

The FCFPS interoperates with external compliance networks and financial-institution APIs through standardized **Trust Verification Requests (TVRs)**. These interfaces support inter-bank or cross-border cooperation while maintaining privacy constraints defined by the UTM.

By embedding cryptographically auditable, privacy-preserving AML/CTF controls within the fabric of the Privacy Network, the FCFPS:

- Eliminates economic incentives for unethical conduct;
- Prevents exploitation of privacy infrastructure for illicit activity; and
- Creates a verifiable bridge between decentralized innovation and global regulatory assurance.

Together, the Privacy-Preserving Compliance System (PPCS) and Financial Crime and Fraud Prevention Service (FCFPS) establish a comprehensive, privacy-native compliance infrastructure that allows lawful innovation and transparent governance to scale globally without compromising confidentiality or regulatory integrity.

4.6 Cross-Organizational Compliance, Ethical Participation & Resource-Pooling

The following sections describe how the foregoing mechanisms interoperate to remove systemic barriers to lawful cross-organizational collaboration and resource reuse.

In conventional economic systems, vast amounts of data, expertise, computing capacity, and intellectual capital remain trapped inside enterprise silos—inaccessible due to privacy, security, fiduciary, or compliance constraints. Even when such collaboration could advance science, sustainability, or economic growth, executives, fiduciaries, and public officials are often legally prohibited from receiving any form of consideration or recognition for their participation.

The invention resolves these limitations by embedding privacy-preserving, compliance-verified governance directly into the technical and legal substrate of collaboration. It

enables lawful, auditable, and confidential participation in shared processes, markets, and data environments—turning compliance itself into the mechanism that ensures trustworthy cooperation.

At its foundation, the framework integrates four interlocking mechanisms:

1. **Quantum Privacy Cells** – legally recognized, limited-liability governance compartments that can be instantiated, operated, and verified under confidentiality and deferred activation;
2. **Proof-of-Trust (PoT)** – a cryptographic verification layer that validates lawful participation, regulatory eligibility, policy compliance, and ethical clearance;
3. **Privacy-Preserving Compliance Service (PPCS)** – an automated, continuous mechanism for enforcing fiduciary, employment, policy, regulatory, and ethics requirements without exposing personal or proprietary data; and
4. **Restricted Derivative Rights (RDR) / Public-Benefit Derivative Rights (PBDR)** – allocation structures that automatically redirect restricted or unclaimable value toward compliant participants or verified public-benefit programs.

Together, these systems form a self-funding, compliance-verified collaboration fabric that converts what were previously legal barriers into engines of lawful, transparent innovation.

4.7 Zero-Marginal-Cost Pooling and Dual-Use Infrastructure

A core advance of the invention is the ability to enable zero-marginal-cost pooling and reuse of existing "dual-use" infrastructure and resources—including data networks, APIs, software platforms, legal contracts, regulatory registries, and human expertise—to both implement and operate the Quantum Privacy Exchange, without requiring new intermediaries or centralized ownership.

Each participant may connect their **Personal Privacy Network (PPN)** or **Enterprise Privacy Network (EPN)** to the ecosystem via existing interfaces and APIs in a way that relies upon, aligns with, or complies with existing legal agreements, licensing rights, and governance mechanisms. These connections allow lawful interoperation between legacy systems while maintaining privacy, data-residency, and fiduciary protections. Each PPN or EPN is associated with one or more Quantum Privacy Cells, which act as autonomous, limited-liability contracting agents. A Quantum Privacy Cell can engage in verified data exchange, service execution, or resource contribution under existing contractual and statutory rights. Because these entities operate under deferred-activation and Proof-of-Trust verification, collaboration remains confidential and compliant until eligibility is confirmed.

This dual-use structure allows the same asset or resource—such as a database, model, or workflow—to be reused across many collaborations simultaneously, each within its own encrypted, auditable context. The marginal cost of adding new lawful participants approaches zero. The result is an exponential-scale reuse economy in which privacy-preserving trust proofs replace manual due diligence, and value compounds with every additional participant.

Lawful Participation and Open-Source Collaboration Framework

The following sections (§§ 3.16 – 3.20) describe how the Quantum Privacy Exchange (QPX) and its Quantum Privacy Accelerators (QPAs) enable lawful, privacy-preserving participation across all roles, sectors, and jurisdictions. Together they define the social, legal, and economic foundations of the **Quantum Privacy participation model**, where individuals, enterprises, and governments collaborate through deferred-activation safeguards, Proof-of-Trust (PoT) verification, and unified policy enforcement under the Unified Trust Model (UTM).

This framework extends the open-source paradigm to regulated collaboration: every verified contribution, dataset, or innovation is cryptographically attributed, rewarded, and lawfully auditable through Quantum Privacy Tokens (QPTs) and derivative rights. In doing so, the QPX transforms compliance, privacy, and ethics from static obligations into engines of coordinated innovation and equitable value creation across society.

4.8 Universal Viral Adoption Model

Within the Quantum Privacy Exchange, every participant operates through a verified Quantum Privacy Cell (QPC) or corresponding Series structure that defines their lawful scope of participation and benefit eligibility. These mechanisms ensure that corporate executives, government officials, investors, consultants, researchers, educators, and citizens can all contribute knowledge, resources, and advocacy safely and ethically—without risk of inducement, conflict of interest, or privacy breach. Each role's participation is governed by Proof-of-Trust verification, deferred activation, and automated redistribution safeguards, ensuring continuous compliance and transparent attribution across the entire ecosystem.

The Quantum Privacy Exchange (QPX) provides the value-distribution layer of this ecosystem. It tracks verified participation, resource contribution, and reuse, issuing QPX Tokens or equivalent rights that represent fractional shares of the aggregate efficiency and social value created. Through integration with the Proof-of-Trust framework and the Privacy-Preserving Compliance System (PPCS), rewards are emergent outcomes of verified collaboration—generated automatically by network effects. Every time a dataset,

workflow, or legal right is reused within compliance boundaries, new measurable value is created and shared.

Because rewards derive from verified system-level efficiency gains rather than direct private transfer, no participant faces a conflict of interest in advocating adoption or interoperability. Executives, fiduciaries, and public officials can promote privacy-preserving infrastructure without violating ethics or procurement laws, as benefits accrue equitably and transparently to the ecosystem as a whole. Early adopters and facilitators receive proportionally higher returns, reflecting and appropriately rewarding their contribution to network growth. Individuals restricted from profiting in their official capacity may still earn a share of secondary or emergent value—captured through personal Quantum Privacy Cells that represent verified, non-conflicted participation in the broader reuse economy.

The PPCS continuously monitors active and pending engagements to detect conflicts or prohibited interests. When an issue arises, the system automatically: (1) reclassifies affected allocations as Restricted Derivative Rights (RDR); (2) flags the associated QPC or Series for suspension, substitution, or adaptive remediation; (3) redirects restricted value to a compliant substitute participant or to a PBDR pool; and (4) identifies alternative compliant resources or workflows to complete the process lawfully. These adaptive substitution mechanisms maintain continuity even as laws or network composition evolves, ensuring collaboration proceeds only with verified participants and lawful provenance—without revealing confidential information.

Illustrative Role-Based Operations

- **Corporate Executives and Employees:** Contribute expertise, relationships, or leadership through Manager-Originated or Manager-Sponsored QPCs while preserving trade-secret protection and fiduciary integrity. Deferred activation and dual-use deployments prevent conflicts of interest or unlawful inducement, while RDR/PBDR safeguards redirect contingent rights to compliant beneficiaries or public-benefit allocations.
- **Government and Elected Officials:** Participate through designated public-benefit QPCs whose economic rights flow automatically to authorized agencies or public trusts—enabling lawful innovation while maintaining compliance with anti-bribery, procurement, and ethics statutes. Officials may also contribute in their personal capacity, independently of their official roles, through separate, deferred-activation QPCs.
- **Venture Investors and Institutional Partners:** Engage through portfolio-linked Quantum Privacy Accelerators (QPAs) that share returns based on verified

contributions and measurable impact—without breaching LP restrictions or fiduciary duties. Accelerator Tokens (ATs) may lawfully recognize advocacy, referrals, or ecosystem development while remaining distinct from regulated financial instruments.

- **Consultants, Lawyers, and Auditors:** Participate transparently while preserving independence and confidentiality. Compliance-verified compartments segregate advisory activities from participation benefits, ensuring full conformance with professional-conduct and conflict-of-interest standards.
- **Engineers, Scientists, and Researchers:** Contribute code, models, datasets, or research findings through privacy-preserving QPCs that guarantee intellectual-property attribution, provenance, and lawful reuse. Verified contributions are automatically tokenized and rewarded under Proof-of-Trust attestation, establishing a transparent, auditable framework for collaborative innovation across academia, industry, and government.
- **Educators, Advocates, and Civil-Society Participants:** Receive lawful recognition and measurable value for outreach, education, and facilitation through Quantum Privacy Tokens (QPTs) or EasyAccess Reward Tokens (EARTs) based on verifiable impact and social benefit—never promotional inducement.

Each act of verified participation amplifies the value of every other participant's contribution—transforming collaboration into a self-reinforcing engine of viral, exponential adoption.

These lawful participation models naturally extend into a universal framework for advocacy and measurable social impact—the Universal Influencer Model.

5. Universal Innovator Model and Impact-Driven Participation

The **Universal Innovator Model** establishes a framework through which any individual, enterprise, institution, or government can participate in the **Quantum Privacy Exchange (QPX)** by contributing verifiable innovation, resources, or expertise.

Instead of rewarding visibility or promotion, the model recognizes demonstrable creation of value—new knowledge, validated data, computational outputs, intellectual property, and trusted relationships—each authenticated through the **Proof-of-Trust (PoT)** system.

Under this model, **innovation and engagement become measurable asset classes.**

Contributors are issued **Resource Tokens (RTs)** or **Exchange Tokens (EXCH)** that reflect their verified impact across participating **Accelerators, Resource Pools,** and **Exchange Networks.**

Every contribution—whether research, software, influence, governance, contractual rights, or capital allocation—is linked to a **Quantum Privacy Cell (QPC)** that anchors lawful ownership, attribution, and revenue participation.

This ensures that innovators—whether individuals or enterprises—retain ownership of their work and resources while participating in federated markets that redistribute verified value transparently and in compliance with fiduciary, privacy, and commercial standards.

The Universal Innovator Model transforms traditional innovation ecosystems into **inclusive, self-funding value networks.**

By unifying invention, validation, and monetization under the **Unified Trust Model (UTM),** it enables innovators to collaborate across sectors and jurisdictions without surrendering control of their data or intellectual property.

Enterprises, governments, and institutions can co-develop solutions, fund verified impact, and procure **innovation-as-a-service** directly from trusted contributors—without intermediaries or opaque licensing structures.

Through this architecture, the **Quantum Privacy Exchange democratizes innovation itself:**

- **Individuals** gain a lawful pathway to monetize creativity, expertise, data, influence, and engagement.
- **Enterprises** gain access to compliant, auditable innovation pipelines that accelerate product and policy development.
- **Governments and public institutions** gain the ability to direct capital toward measurable social outcomes while maintaining transparency and accountability.

By adopting the Quantum Privacy Network to streamline operations and engage with their ecosystems, enterprises and public institutions can simultaneously streamline processes, eliminate bureaucracy, and slash waste and costs through the **zero-marginal-cost reuse, free-market efficiencies, and verified value generation** the system produces.

The public sector thus becomes both a **beneficiary and a catalyst** of the Universal Innovator Model—demonstrating that privacy, accountability, and fiscal responsibility can reinforce rather than constrain one another, and replacing taxes with self-funding networks.

Economically, the model integrates with the **Quantum Privacy Treasury Layer (§8)** to enable continuous reinvestment of verified impact into new innovation cycles. Revenues, token distributions, and derivative rights flow automatically to innovators and their affiliated Accelerators through governed smart contracts and PoT-verified attribution.

In essence, the Universal Innovator Model replaces passive influence with **active, measurable contribution**—transforming innovation into a **trust-verified public utility** that advances economic inclusion, sustainability, and collective prosperity.

5.1 Transitioning from the Influencer Economy to the Innovator Economy

The **Quantum Privacy Exchange (QPX)** redefines the economics of digital engagement. It transforms the **social-media influencer economy**—which today monetizes attention, emotion, and addiction—into a **Universal Innovator and Impact Economy** that rewards measurable creativity, insight, and positive behavioral change.

In the traditional social-media model, value is extracted from users' time and data. Engagement is optimized for compulsion and controversy, rewarding the beautiful, the provocative, the divisive, and the famous. Influence is measured by visibility rather than substance, and advertising revenues depend on driving consumption rather than improvement.

The **Universal Innovator Model** reverses that dynamic. It empowers every participant—not just influencers—to contribute what they uniquely create or enable: intelligence, initiative, empathy, expertise, relationships, and imagination. Within the Quantum Privacy ecosystem, **advocacy and engagement themselves become public goods**. In this model, **innovation and positive engagement replace attention as the source of value**, and every verifiable act of contribution, education, or problem-solving becomes a measurable unit of impact within the Quantum Privacy Exchange.

The **Quantum Privacy Exchange (QPX)** provides a **lawful, auditable pathway** for social-media platforms, content networks, and advertising ecosystems to evolve beyond their dependence on **targeted advertising and behavioral manipulation**.

By integrating **Quantum Privacy Networks (QPNs)** and **Proof-of-Trust (PoT)** verification—often with **minimal technical effort or cost**—these platforms can **repurpose their existing user bases, engagement tools, and data infrastructures** into **multi-sided innovation marketplaces**, where the same audiences, algorithms, and interfaces now drive **measurable gains in health, education, productivity, and sustainability**.

Even if these vendors initially choose not to participate directly, their **advertising, e-commerce, social-media, and clean-room infrastructures**—along with their **digital content, installed bases, and revenue flows**—can still be **harnessed and monetized by their customers and users** as **dual-use resources** through multiple pathways.

Existing posts, content, messages, and engagement surfaces can be activated through automatically generated **EasyAccess Links** and derivative content, enabling users to route attention and engagement directly into QPN workflows. **EasyAccess Messaging** allows individuals and enterprises to reuse their existing messaging channels (SMS, email, social

DMs, group chats, comment threads, etc.) as privacy-preserving orchestration surfaces for referrals, coordination, and impact-driven engagement. And for developers and enterprises that wish to enable their systems natively, the **EasyAccess Consent API** provides a lightweight, platform-independent way to embed EasyAccess authorization natively into apps, websites, clean rooms, advertising networks, and enterprise services—instantly making them discoverable, linkable, and orchestratable within the Privacy Exchange Exchange without requiring platform approval, new integrations, or data-sharing agreements.

This enables users and enterprises to **recycle existing engagement channels** into the operational fabric of the QPX—**powering adoption and value creation** without requiring platform approval or disrupting current business models.

In this new paradigm, a platform's **core revenue streams shift** from advertising and impulse commerce to **verified innovation, knowledge transfer, and outcome-based services**.

Engagement becomes the **input for positive transformation**: users, creators, educators, and enterprises collaborate within a **privacy-preserving environment** where every contribution is **verified, auditable, and equitably rewarded**.

Crucially, this transition is not only **more sustainable**, but **vastly more lucrative**. The QPX replaces the finite and extractive economics of attention monetization with an expansive, compounding system of verified impact and innovation—**transforming today's trillion-dollar, advertising-driven attention economy into an Innovator and Impact Economy exceeding tens of trillions globally.**

By removing the dependency on advertising as the primary revenue source, **platforms gain a durable, structural alignment with the AI agent–based business model they already aspire to—one in which intelligent agents act autonomously on behalf of users, creators, and enterprises**, transacting value directly through Proof-of-Trust and tokenized outcome exchanges. In this model, the QPX becomes the missing economic substrate for next-generation autonomous-agent ecosystems, providing both the revenue architecture and societal alignment that current AI systems lack. The result is a transformative shift from attention extraction to verifiable impact creation—unlocking a far more scalable, ethical, and profitable foundation for the digital economy.

This evolution eliminates the **perverse financial incentive** to algorithmically amplify addictive, polarizing, or destructive content—ending one of the most damaging feedback loops in modern economic history.

Instead of rewarding outrage and division, the QPX rewards **verified creativity, knowledge, productivity, social contribution**, restoring economic alignment between what benefits individuals and the society and what sustains the platform ecosystem.

Platforms that once monetized **distraction and attention** can now monetize **well-being, learning, and productivity**—unlocking far greater **economic and social value** while maintaining full compliance with **privacy, fiduciary, and regulatory frameworks**.

Through this transformation, **social platforms and advertisers not only preserve but multiply their relevance and profitability**.

Their **advertising networks** evolve into **innovation and impact networks**; their **user analytics** become **Proof-of-Trust metrics**; and their **targeted campaigns** transform into **outcome-based participation programs** that generate **recurring, verifiable value** for users, partners, and shareholders alike—anchored in trust, privacy, and measurable progress.

In macroeconomic terms, the **Quantum Privacy Exchange (QPX)** transforms today's **$1.2 trillion global advertising economy**—largely built on monetizing attention, surveillance, and addiction—into **more than $10 trillion** of **Verified Innovation and Impact Economy** anchored in measurable social and economic progress.

By redirecting the world's digital-engagement infrastructure toward **health, education, productivity, and sustainability**—and enabling AI to drive positive change across the economy and society—the QPX unlocks a **new class of lawful, asset-backed economic growth**. This growth compounds across industries, markets, and jurisdictions.

Each conversion of attention into verified innovation becomes a durable source of GDP expansion and wealth creation, **transforming the world's most powerful behavioral systems from extractive engines of distraction into regenerative engines of collective prosperity**. Within the Quantum Privacy ecosystem, advocacy and engagement are elevated into public goods.

Participants are **recognized and rewarded** not for driving consumption, but for producing **measurable, verifiable improvements** in individual and collective outcomes and productivity. **Proof-of-Trust (PoT)** ensures that every act of advocacy, facilitation, or collaboration remains **ethical, auditable, and privacy-preserving**, while **Quantum Privacy Tokens (QPTs)** and **EasyAccess Reward Tokens (EARTs)** provide **transparent, proportional recognition** for verified outcomes.

You can't improve what you can't measure—and you can't reward what you can't verify. That principle hasn't changed. What Quantum Privacy changes is the feasibility of applying it. The **Quantum Privacy Network (QPN)** and the **Quantum Rating Metrics make**

it possible to measure anything and reward anyone—ethically, privately, and without surveillance or disclosure. (See § 8 for more detail.)

By enabling privacy-preserving, outcome-based measurement and verifiable attribution, QPN transforms real-world positive behavior into a secure, distributable source of economic value. Every verified act of creativity, collaboration, or improvement becomes part of an auditable impact ledger that drives both social and financial returns across the Quantum Privacy Exchange (QPX).

Examples of Impact-Driven Innovation

- **Health and Well-Being Impact**
  Individuals and communities that **inspire healthier habits and stronger relationships, or help their friends and neighbors in need** earn **EasyAccess Rewards** or other **Quantum Privacy Tokens (QPTs)** tied to verified indicators of improvement—such as higher preventive-care adherence, better nutrition, improved fitness, or reduced stress—**without revealing a single piece of personal data**.

  Whether it's a family that supports each other in meeting wellness goals, a community that embraces preventative care, or an influencer who motivates positive change, **Quantum Privacy transforms compassion and accountability into measurable, tradable value**.

- **Education and Knowledge Advancement**
  Teachers, mentors, journalists, and thought leaders who **expand understanding, curiosity, and critical thinking**—and who help individuals achieve better employment, educational, and life outcomes—are recognized for producing verified learning and engagement impacts.

  The **Quantum Privacy Exchange (QPX)** quantifies these contributions transparently, linking value directly to **knowledge creation, literacy, and intellectual growth, all without surveillance or data extraction**.

  Examples include educators who make learning fun and relevant; mentors whose encouragement keeps students engaged; journalists who clarify rather than polarize; and thought leaders who use their platforms to **inform, unite, and inspire rather than inflame or divide.**

  In this model, teaching, mentoring, and communication become **verifiable engines of social and economic value**. Every act of shared insight or understanding generates measurable returns—**turning the pursuit of knowledge into a regenerative force for prosperity, fairness, and trust**.

- **Sustainability and Civic Innovation**

  Organizers, educators, entrepreneurs, and citizens who **champion sustainability, transparency, and civic participation** earn **tokens for verified progress**—reduced energy use, cleaner supply chains, higher recycling rates, improved public safety, or enhanced community well-being—**all verified through privacy-preserving aggregation and Proof-of-Trust attestations**.

  Each measurable step toward sustainability becomes both an **economic signal and a social dividend**, transforming climate and civic responsibility from a moral aspiration into an **auditable, revenue-generating asset class** within the Quantum Privacy Exchange.

- **Enterprise and Workforce Transformation**

  Employees, executives, and innovators advancing **ethical AI, secure data collaboration, or accountable automation** accrue **deferred rewards** through **Quantum Privacy Cells (QPCs)** tied to verified gains in **productivity, fairness, and compliance**.

  Each verified improvement—fewer errors, better outcomes, greater efficiency—feeds directly back into the **Proof-of-Trust framework**, producing measurable **efficiency dividends, reputational capital, and shared prosperity** across participating enterprises.

  Within the QPX, ethical innovation isn't just good governance; **it becomes a measurable competitive advantage that compounds over time.**

Each of these activities generates **quantifiable, privacy-preserving gains** in knowledge, well-being, and social trust—outcomes that **Quantum Privacy** can **measure, verify, and reward ethically** through **QPTs**, **EasyAccess Rewards**, and **derivative token rights**.

Together, these verified actions form the **microeconomic foundation of the Universal Innovator Model**, turning positive human and organizational behavior into a **trusted, tokenized engine of value creation**.

5.2 Universal Influencer Model: Celebrity Catalysts and Viral Adoption

As verified advocacy scales across individuals, enterprises, and communities, the next phase of adoption depends on **cultural amplification**—the ability to translate verified impact into shared aspiration.

Here, **cultural leaders and public figures** become essential catalysts, accelerating the transition from passive engagement to purposeful participation. By embodying and promoting measurable social progress, they transform innovation into a shared cultural narrative—one that unites audiences around **trust, creativity, and positive impact**.

Celebrity influencers, musicians, athletes, and cultural, political, scientific, and business thought leaders serve as pivotal catalysts in the **Universal Influencer Model**—transforming the reach of social media into a regenerative engine of privacy-preserving engagement and measurable positive impact.

Through the **Quantum Privacy Exchange (QPX)**, these figures can mobilize their existing audiences to join the **Quantum Privacy Network (QPN)** instantly and lawfully via **EasyAccess** links, and EasyAccess-enabled apps and content.

Each EasyAccess-enabled post, stream, message, or campaign can automatically establish **Personal Privacy Networks (PPNs)** and corresponding **Quantum Privacy Cells (QPCs)** for every participating fan or follower. These personal compartments grant each individual better privacy, stronger security, and continuous control over how their data, identity, and digital interactions are used for free—while also earning them a share of the value they help create through **EasyAccess Rewards** and **QPX Tokens**.

Engagement of any kind—accessing a secure message, opening an article, installing an app, or reserving a concert ticket—becomes **universally valuable** across domains. What begins as simple fandom extends into a lifetime relationship that improves each participant's digital life: optimizing healthcare, enhancing education and work skills, increasing productivity, and improving financial and e-commerce outcomes.

For influencers and content creators, the rewards are amplified when their audiences' engagement leads to **verified positive behavior change**—healthier habits, stronger communities, improved learning, and sustainable lifestyles. Each measurable improvement is authenticated through **Proof-of-Trust (PoT)**, transforming every act of influence into a quantifiable contribution to social and economic well-being.

Unlike today's impulse-commerce model that commoditizes attention, **EasyAccess** converts engagement itself into a durable, revenue-generating asset. For high-profile influencers, the upside is **orders of magnitude greater** than traditional sponsorships, because value compounds through verified impact, recurring participation, and universal adoption.

5.3 Universal Platform Adoption: Social Media as Global QPC Networks

Social media and online platforms can **convert their entire user populations into a global network of QPCs with minimal effort**—simply by updating the language in their privacy policies and submitting user consents asynchronously to the **EasyAccess Consent API.** Because the API is built on ubiquitous **OAuth 2.0** principles but does not require user-facing redirects for existing consent records, most platforms can enable full QPC activation within a single day of engineering effort—without affecting system performance, user experience, or operational stability.

Once implemented, these platforms can leverage **AI-generated viral EasyAccess Links and EasyAccess-enabled Apps and Content** to organically expand participation—repurposing their existing digital populations, data, infrastructure, content, and engagement algorithms to grow to the entire global population at **zero marginal cost**.

Every user interaction becomes a verified, privacy-preserving point of value creation, seamlessly aligned with lawful consent and measurable impact.

Influencers, creators, platform vendors—or virtually anyone—can form **self-organizing, self-funding Social Accelerators** that operate as unified, omni-channel **EasyAccess Engagement Networks**.

These Social Accelerators aggregate audience engagement, brand collaborations, and verified advocacy into cohesive ecosystems—functioning as some of the **most lucrative Exchange Networks** within the QPX.

Each network operates transparently under the **Quantum Privacy LLC Series** structure, leveraging the **Quantum Privacy Cell Participation Agreements** to anchor ownership, revenue sharing, and governance among participants.

This architecture allows the network to grow **virally and autonomously**, funding its own launch and expansion even before the Quantum Privacy Exchange is fully operational.

Because participation is tied to verifiable introductions, endorsements, and referrals, even simple actions—such as sharing an Accelerator invitation via email or social post—can retroactively trigger value creation and **tokenized attribution through QPX Tokens and derivative rights**.

The result is **passive viral growth at zero marginal cost**: every social connection becomes a potential trust node, every endorsement a financial instrument, and every community a self-sustaining micro-economy.

5.4 EasyAccess: The Engine of Viral Growth

The **Universal Adoption Model** makes this growth self-propagating.

EasyAccess Links—or EA-enabled content—can be embedded anywhere or distributed through any channel: emails, websites, social posts, mobile apps, messaging clients, or AI chatbots.

Users or systems can generate these links in seconds through the **EasyAccess Link Builder** or the **EasyAccess Link API**. Enrollment is nearly frictionless—the only visible change may be updated privacy-policy language.

A single celebrity campaign can ignite **cascading global adoption**, enrolling millions or billions of participants who each receive their own PPN and QPC, all while generating compounding residual rewards for the initiator.

Importantly, **EasyAccess Rewards can be self-funding from the outset** by reusing existing affiliate-marketing, advertising, and e-commerce infrastructures. This enables creators, influencers, and participants to benefit immediately—long before the full QPX architecture is deployed—making adoption both **viral and profitable from day one**. As these rewards propagate, they grow highly lucrative EasyAccess Engagement Networks that can operate across any market and seamlessly cross-fertilize with any other Exchange Network.

Together, these mechanisms redefine celebrity influence as a **universal force for measurable social progress**—uniting economic incentives, cultural capital, and ethical impact within a single, trust-verified system. Ubiquitous adoption is inevitable and unstoppable – the only question is, how will the EasyAccess Rewards and QPX Tokens be allocated, and which people and which tech platforms will lead the revolution.

(See also § 4.7, "Universal Viral Adoption Model," for the foundational mechanics of viral propagation, and § 5.1, "From Social Influence to Verified Impact," for the behavioral and economic framework underlying EasyAccess engagements.)

5.5 Lawful Participation, Dual-Use Collaboration & Self-Funding Adoption

The Quantum Privacy Exchange (QPX) and Quantum Privacy Accelerators (QPAs) establish a unified participation model that allows individuals, enterprises, and institutions to contribute lawfully, ethically, and transparently—without breaching fiduciary, employment, or regulatory obligations. All participation occurs under the Unified Trust Model (UTM) and Proof-of-Trust (PoT) verification framework, ensuring that every contribution, benefit, or derivative right is verified for compliance before activation.

Open-Source and Dual-Use Equivalency

Participation within the QPX is legally and ethically equivalent to contributing to an open-source or public-benefit ecosystem. Contributions—whether data, software, expertise, or policy logic—may be personal, enterprise-sponsored, or agency-supported; all are voluntary, non-exclusive, and dual-use in nature. Each input is recorded under privacy-preserving NDAs and the UTM, guaranteeing IP control, provenance, and lawful reuse.

Verified datasets, workflows, and governance modules are recombinable under cryptographic provenance, generating cumulative efficiency and measurable social value. These verified outputs are tokenized through Quantum Privacy (QP) Tokens and derivative rights, distributing recognition and reward lawfully across all contributors.

For detailed role-based examples of how these mechanisms apply across sectors, see § 3.16 (Lawful Participation Models and Role-Based Applications within the QPX Ecosystem)

Deferred Activation and Conflict-Free Compensation

Manager-Originated or Manager-Sponsored Quantum Privacy Cells (LLC Series) confer no ownership, compensation, or obligation until verified compliance is complete. All potential conflicts of interest are automatically diverted into Public-Benefit Derivative Rights (PBDR) pools or reassigned to compliant proxies through Proof-of-Trust-verified provenance, eliminating unlawful inducement and preserving fiduciary integrity.

These safeguards ensure that every contribution—personal or institutional—operates under verifiable ethics, lawful delegation, and zero-coercion incentives.

Lawful Personal-Capacity Advocacy and Freedom of Expression

Individuals may advocate for or contribute to the Quantum Privacy ecosystem in their personal capacity—independently of their employment, fiduciary, or governmental roles—much like volunteering in an open-source project. This participation is protected under multiple legal and ethical doctrines, including freedom of speech, freedom of association, and whistleblower and employee-protection statutes. **These laws collectively prohibit employers, government agencies, and other institutions—as well as individuals acting in supervisory, managerial, fiduciary, or organizational roles—from restricting or retaliating against lawful, off-duty advocacy conducted without misuse of official resources or confidential information.** Protected expression encompasses speech and association on matters of public concern, including privacy, ethics, and data-governance reform.

For public employees, this protection derives from the **First Amendment** and the **Whistleblower Protection Enhancement Act (5 U.S.C. § 2302(b)(8))**, as interpreted under *Pickering v. Board of Education* and *Connick v. Myers*. For private-sector participants, it arises under the **Sarbanes–Oxley Act § 806 (18 U.S.C. § 1514A)**, **Dodd–Frank Act § 922 (15 U.S.C. § 78u-6)**, and numerous **state labor codes** safeguarding lawful off-duty conduct and political activity (e.g., **Cal. Lab. Code §§ 1101–1102**). Additional protection exists for collective or collaborative engagement under the **National Labor Relations Act § 7 (29 U.S.C. § 157)**. Together, these provisions ensure that advocacy for lawful technological or governance reform—including promotion of privacy-preserving digital infrastructure—constitutes protected expression that cannot lawfully be penalized or suppressed.

Government and elected officials likewise retain the right to engage in personal-capacity advocacy, provided that no official resources or authority are used. Quantum Privacy's **Public-Benefit Series** and **Restricted/Public-Benefit Derivative Rights (RDR/PBDR)** mechanisms guarantee that no personal enrichment can occur, maintaining compliance

with the **U.S. Federal Bribery Statute (18 U.S.C. § 201)**, **FCPA**, **UK Bribery Act 2010**, and **OECD Anti-Corruption Principles**.

In practice, the Quantum Privacy Cell (QPC) architecture makes lawful personal-capacity participation, and deferred token rewards for such contributions, both private and effectively undetectable. Each QPC operates as an encrypted, limited-liability governance compartment that can record contributions, verifications, and tokenized recognitions without revealing the participant's identity, employment, or affiliations. Because Manager-Originated Series are created unilaterally by Quantum Privacy LLC Managers, participants need not acknowledge or even be aware of a Series until activation. Consequently, employers, agencies, and counterparties have **no legal or technical means** to confirm or compel disclosure of participation, as QPC records are protected trade-secret materials under the **Defend Trade Secrets Act (18 U.S.C. § 1836)** and corresponding state laws.

If coercion or discovery is attempted, the **Confidentiality and Protective Reconstitution Policy** empowers Quantum Privacy LLC Managers (or automated agents automating implementation of provisions of the Quantum Privacy LLC's Operating Agreements or policies) to terminate and reconstitute the affected Series, preserving accrued rights under a new confidential identifier and rendering the original record inaccessible. This ensures that individuals can contribute, advocate, and innovate safely—even in restrictive corporate or political environments—while retaining full protection under constitutional, statutory, and contractual law.

Cross-References:
See also **§ 1.3 (Ethical, Fiduciary & Regulatory Constraints)** for governing compliance foundations; **§ 2.2 (Deferred Activation, Proof-of-Compliance, and Delegation of Rights)** for architectural mechanisms; **§ 2.9 (Quantum Accelerator Architecture for Decentralized Innovation)** for participatory mechanisms and self-funding adoption dynamics; and **§ 3.16 (Lawful Participation Models and Role-Based Applications within the QPX Ecosystem)** for extended examples of lawful participation examples across sectors.

5.6 Governance, Compliance, Lifecycle Continuity & Adaptive Reinforcement

Quantum Privacy Cells operate under continuous compliance verification through the Unified Trust Model (UTM) and Proof-of-Trust (PoT) frameworks. Each Series or governance compartment can be automatically suspended, reconstituted, or redirected upon detection of a compliance violation, conflict of interest, or attempted coerced disclosure.

If external pressure or discovery attempts seek to compel identification or disclosure, Quantum Privacy LLC Managers—or their automated agents—may terminate and later reconstitute the affected Quantum Privacy Cell under new credentials while preserving

privacy, provenance, and lawful continuity. **Confidential-Existence** provisions ensure that no participant, institution, or service provider can be compelled to confirm or deny the existence of a Quantum Privacy Cell or its beneficiaries.

Together with the Proof-of-Trust Accelerator, this framework establishes a continuous feedback loop between technical innovation, ethical enforcement, and regulatory compliance. As participation expands and policies evolve, the system automatically updates constraints, redistributes value, and reinforces lawful collaboration—creating an adaptive, self-correcting trust ecosystem that sustains privacy, transparency, and accountability across jurisdictions.

Summary:

By combining lifecycle continuity, confidential reconstitution, and adaptive governance, this mechanism ensures that Quantum Privacy Cells remain lawfully compliant, ethically enforceable, and resilient against coercion or compromise—forming the living backbone of the Quantum Privacy Exchange.

Cross-References:

See also § 2.2 (*Deferred Activation, Proof-of-Compliance, and Delegation of Rights*) for the foundational compliance logic; § 3.8 (*Regulatory and Legal Enablement under the Unified Trust Model and Proof-of-Trust*) for statutory integration; and § 4 (*Quantum Privacy Accelerator Systems and Methods for Self-Funding, Trust-Verified Market Formation*) for the operational layer that implements continuous verification and redistribution across Accelerators.

5.7 Societal & Economic Implications and the Open-Source Economy of Trust

The architecture redefines how value is created and distributed by making privacy, compliance, and ethics intrinsic system properties:

- **Zero-Marginal-Cost Reuse.** Regulated, proprietary, and personal resources become universally reusable under lawful constraints, multiplying their economic and social utility.
- **Inclusive Value Participation.** Any lawful person or enterprise can earn a proportional share of emergent value created by verified resource reuse, regardless of position, employer, or jurisdiction.
- **Dual Incentive Alignment.** Participants who cannot directly profit in their official capacity can still benefit indirectly through personal, compliant QPCs linked to verified public value creation or lawful advocacy outside official roles.

- **Universal Adoption Economics.** QPX Tokens reward all contributors to lawful growth; early adopters accrue amplified returns—so every participant is motivated to expand, evangelize, and contribute to the network.

Unlike traditional open-source ecosystems that rely primarily on goodwill, the QPX embeds tokenized attribution and trust-verified rewards, creating transparent economic incentives to share and reuse valuable resources while preserving privacy, compliance, and ownership. Contributors are recognized and compensated for verified participation, innovation, and advocacy through Quantum Privacy Tokens (QPTs) and derivative-rights allocations. These mechanisms convert collaboration into measurable, auditable economic value—aligning individual motivation with collective benefit while maintaining full regulatory compliance and ethical integrity.

Access for Everyone. The Quantum Privacy Exchange redefines what "access" means. It tears down the walls between capital and creativity, giving anyone with talent and purpose the same reach as today's biggest players. Once at full scale, a kid in Kentucky or Kathmandu will be able to pursue their great idea with the same data, tools, and global reach as today's tech giants—at zero marginal cost and with a fair share of the value created.

This architecture turns compliance from a constraint into a catalyst, enabling every verified reuse, adaptation, or improvement to generate shared value. The result is a planetary-scale, self-sustaining digital commons—an open-source economy of trust—where collaboration, compliance, and social good continuously reinforce one another through cryptographically verifiable exchange and equitable reward.

6. QP Accelerator for Self-Funding, Trust Verified Market Formation

Each **Quantum Privacy Accelerator (QPA)** constitutes a distinct, self-organizing innovation network operating within the broader **Quantum Privacy Exchange (QPX)**. A QPA integrates the **Proof-of-Trust (PoT)** compliance layer, **Quantum Privacy Cells (QPCs)**, and **Quantum Privacy Networks (QPNs)** to enable decentralized innovation, lawful capital formation, and continuous process optimization under verified compliance.

While the term *"Accelerator"* is used interchangeably throughout this specification, the term **Quantum Privacy Accelerator (QPA)** refers specifically to an implementation that provides end-to-end **Quantum Privacy™** and **Proof-of-Trust-accredited** security, privacy, and policy enforcement under the **Unified Trust Model (UTM)**. Early or transitional deployments that rely on existing dual-use technologies or traditional legal agreements—anchored by **Enterprise Privacy Networks** or early **Accelerator Participants**—remain encompassed by the terms *"Accelerator"* or *"Privacy Network Accelerator."*

A QPA can self-organize from inception, beginning with deferred-activation **Quantum Privacy Cells** (legally embodied as **Quantum Privacy LLC Series**, and initially implemented via contribution records and/or legal agreements) that align incentives for individuals and enterprises to pool resources and collaborate. These entities connect existing dual-use infrastructure into **Exchange Networks** and **Resource Pools**, negotiate revenue- and derivative-rights-sharing agreements, define mutually trusted **Trust Criteria** and **Trust Credentials**, and have all such frameworks verified and accredited under the **Unified Trust Model** through the **Proof-of-Trust (PoT) Accelerator**.

Collaborative governance, resource pooling, and derivative-rights allocations among QPA participants are coordinated through **Inter-QPC Agreements**, which—as described in § 3.8—enable privacy-preserving contractual enforcement and cross-organizational coordination without exposing proprietary, regulated, or personal information among participants.

This decentralized model of development, ownership, and funding enables **zero-marginal-cost reuse** of existing infrastructure, legal frameworks, business processes, and resources. It provides an incremental, self-funding adoption path that eliminates the need for large upfront investment while rewarding early innovators with sustainable first-mover advantages—advantages that convert into tokenized ownership rights as the **Quantum Privacy Exchange (QPX)** reaches critical mass and their **Quantum Privacy Cells (QPCs)** activate.

Subsequent sections describe how **Quantum Privacy Accelerators** autonomously create liquidity, tokenize verified resources, and allocate revenue through **compliance-verified governance events**, forming the functional and economic core of the **Quantum Privacy Exchange (QPX)** ecosystem.

Limitations of Legacy Innovation and Capital Formation Models

Modern innovation ecosystems—spanning venture capital, private equity, corporate innovation programs, and government funds—remain structurally inefficient and exclusionary across most jurisdictions and technology stacks. They depend on large, sequential, capital raises, manual compliance processes, and limit participation to privileged insiders concentrated within elite networks and innovation hubs. The effective cost of capital often exceeds 25–40%. At the same time, consensus-driven governance and reliance on conservative Limited Partners reinforce herd behavior in “hot” sectors, rather than enabling truly disruptive innovation.

These legacy models exclude the vast majority of the world’s potential innovators—particularly those operating in regulated sectors, public institutions, or developing markets. Legal, fiduciary, and compliance barriers prevent cross-organizational pooling of

data, infrastructure, and expertise, leaving billions of people and trillions of dollars in underutilized assets trapped within institutional silos.

Traditional venture investing is also poorly suited to capital-intensive or high-compliance innovation—such as artificial intelligence, which now requires hundreds of billions to trillions in cumulative investment—or to adoption in enterprise, governmental, or privacy-sensitive domains such as healthcare, finance, or education.

The result is a global innovation engine that is costly, inequitable, and slow—and, paradoxically, not particularly innovative. Only a fraction of human and natural capital participates in efficient markets, while most of the planet's intellectual property, data, and ecological value remain isolated, underleveraged, and excluded from lawful, transparent monetization.

The present invention democratizes access to finance, innovation, and ownership. Through privacy-preserving legal-technical frameworks—such as the Quantum Privacy Exchange (QPX) architecture or functionally equivalent systems that integrate confidential entity structures, compliance verification, and tokenized exchange mechanisms—any individual, enterprise, or institution, regardless of geography, wealth, or technical sophistication, can participate directly in the innovation economy.

Within the Quantum Privacy Exchange, **everyone becomes a shareholder, everyone an entrepreneur, and the entire world our market, our workforce, and our distribution network.** This redefines global capitalism as a participatory, person-centered system in which inclusion, fairness, and opportunity are not afterthoughts, but intrinsic design principles.

Although the preferred embodiment employs the Quantum Privacy Exchange (QPX), Quantum Privacy Cells, and Proof-of-Trust™ frameworks developed by WebShield, Inc., equivalent embodiments may utilize any privacy-preserving, compliance-verified coordination fabric that achieves substantially the same functions of lawful participation, automated compliance, and tokenized liquidity formation.

6.1 Architecture & Core Mechanisms

Quantum Privacy Accelerators ("Accelerators") transform innovation from a speculative, capital-intensive pursuit into a self-funding, compliance-verified, and liquidity-enabled exchange—providing **zero-marginal-cost, open access** to the resources required to develop, deploy, operate, and distribute new networks, products, and services.

Each Accelerator functions as a **domain-specific orchestration engine—a "meta-venture"** that unifies legal enforceability, cryptographic privacy, and automated compliance within a single operational fabric. Resources from any lawful source—public,

private, or personal—can interoperate seamlessly across organizations, industries, and jurisdictions while preserving verifiable compliance, provenance, and accountability.

Equivalent embodiments may be realized using any privacy-preserving or compliance-verified infrastructure that integrates:

- **Confidential entity governance** – e.g., limited-liability compartments or regulated custodial entities;
- **Automated compliance validation** – such as policy-based attestations and fiduciary-verification mechanisms; and
- **Programmable liquidity frameworks** – including tokenized or contract-based revenue- and rights-distribution mechanisms.

Because **Quantum Privacy™, Proof-of-Trust™, and the Unified Trust Model™** are inherently technology-, topology-, and vendor-neutral, they can extend trust, privacy, and governance capabilities to any existing or future infrastructure, trust framework, or resource—rendering them **dual-use assets** available at zero marginal cost via Personal or Enterprise Privacy Networks.

Disparate networks or platforms—even those operating independently or in apparent competition with the Quantum Privacy Exchange—can interconnect so that they continue to function under their existing business practices and revenue models **while simultaneously enabling and generating incremental revenue through the Quantum Privacy Exchange**. This dual-use operation can occur transparently, utilizing existing APIs, interfaces, legal agreements, and governance structures **without requiring detectable integration, disclosure, or approval.**

By enabling dual-use infrastructure and resources, this architecture not only **drastically reduces the cost of incubating Accelerators** but also ensures that **institutional inertia and entrenched incumbents cannot impede adoption.** In short, resistance is futile—**all can be empowered by Quantum Privacy™, whether they realize it or not.**

Core Mechanisms

1. **Confidential, Limited-Liability Governance Compartments** — Legal-technical entities (e.g., Quantum Privacy Cells or functionally equivalent compartments) that represent participants and their verified rights; provide ring-fenced liability; and support deferred activation and auditable participation without public disclosure.
2. **Personal and Enterprise Privacy Networks (PPNs/EPNs)** — Privacy-preserving participation layers that connect individuals, enterprises, and institutions via existing APIs, contracts, and regulatory frameworks, enforcing consent, trust, and compliance end-to-end across distributed infrastructures.

3. **Quantum Privacy Exchange (QPX) or Equivalent Universal Settlement Layer** — A global marketplace and liquidity backbone that tracks, verifies, and settles value created through lawful resource reuse and collaboration, supporting instantaneous, compliance-verified settlement across human, digital, and ecological assets.
4. **Resource Tokens (RTs)** — Cryptographic representations of ownership, provenance, and usage rights for regulated or proprietary resources—data, content, software, compute, contracts, or IP —preserving value and attribution across repeated lawful reuse.
5. **Accelerator Tokens (ATs)** — Fractional participation rights reflecting verified contributions and outcomes within an Accelerator's domain, which may be automatically issued under **Proof-of-Trust (PoT)** validation and forming the foundation for equitable, auditable value distribution.
6. **Exchange Networks** — Governed marketplaces that syndicate RTs and ATs into interoperable markets. Exchange Networks define trust criteria, attribution logic, and revenue-allocation mechanisms, enabling lawful, transparent trade of tokenized value across domains.
7. **Liquidity Pools** — Compliance-verified treasury mechanisms that securitize and circulate verified token flows across sectors, providing early and continuous liquidity for participants and linking tokenized rights to fiat, stablecoins, or real-world-asset (RWA) instruments.

Integration with the Quantum Privacy Exchange (QPX)

The **QPX** serves as the **global settlement and liquidity backbone** for all Accelerators and participating entities. Within this framework:

- The **Unified Trust Model (UTM)** and **Proof-of-Trust (PoT)** embed regulatory, contractual, and ethical constraints directly into token and transaction logic, ensuring compliance from creation to redemption.
- **Resource Tokens** encode long-lived ownership, provenance, and usage rights, persisting across decades of lawful reuse.
- **Exchange Networks** and **Resource Pools** organize participants and their tokenized resources into governed markets that define interoperability, pricing, and attribution.
- **Liquidity Pools** provide continuous capitalization, hedging, and conversion—transforming deferred or illiquid token streams into circulating assets that can fund ongoing innovation.

Together, these components create a **universal, privacy-preserving market infrastructure** that automates trust, reduces friction, and enables **self-funding, zero-marginal-cost participation** in the global economy. By embedding compliance, auditability, and liquidity into the structure of collaboration itself, Accelerators:

- **Democratize access** to finance, innovation, and ownership;
- **Align incentives** among individuals, enterprises, and governments;
- **Unlock siloed assets** (data, IP, infrastructure, and institutional capacity); and
- **Turn privacy and regulation** from constraints into engines of equitable growth and global coordination.

This system replaces hierarchical, capital-intensive structures with an adaptive, lawful, and self-reinforcing network economy—where participation is a right, not a privilege, and **verified contribution becomes the universal currency of value**.

6.2 Accelerator Classes, Legal Forms, and Incentive Alignment

Each **Accelerator** functions as a distributed, compliance-verified exchange network established for a specific purpose, theme, or constituency. Accelerators may be thematic or sector-based—such as those operated by the **EP3 Foundation**, including *Quantum Privacy & AI*, *Healthcare (Lōkahi)*, *Agentic Finance & Commerce*, *Sustainable Markets*, *Online Child Safety*, and *Education & Workforce Development*. Alternatively, Accelerators can be formed on behalf of specific enterprises, industries, investment firms, geographies, or social missions. Illustrative variants include:

- **Enterprise & Startup Accelerators** — Created by companies or joint ventures to tokenize innovation pipelines and globalize compliant collaboration.
- **National & State Accelerators** — Operated by public institutions or economic-development agencies to promote privacy-preserving, self-funding innovation ecosystems.
- **Portfolio Accelerators** — Established by venture-capital firms, family offices, sovereign-wealth funds, or private-equity sponsors to orchestrate cross-portfolio synergies and share liquidity through Quantum Privacy Liquidity Pools.
- **Social Accelerators** — Initiated by associations, advocacy groups, philanthropies, creators, or community networks to fund public-interest or mission-driven programs using lawful tokenized participation.
- **Platform, Application, and Market Accelerators** — Supporting interoperable data, AI, and marketplace infrastructure across multiple industries and jurisdictions.

Legal and Organizational Forms

Accelerators may be implemented as specialized **confidential limited-liability entities**—such as a **Quantum Privacy Cell**, **Series LLC**, **Foundation**, or **Protected Cell Company**—or any equivalent legal structure that provides ring-fenced liability, privacy-preserving governance, and audit-ready compliance. They may optionally be instantiated through **automated, compliance-verified formation APIs** or direct integrations with jurisdictional registries.

Early-stage deployments may begin as streamlined entities (for example, **Delaware Series LLCs**) for modular scalability and later reconstitute into alternative legal forms—such as **Delaware C-Corporations**, **Cayman Foundations**, **Segregated Portfolio Companies (SPCs)**, or **Incorporated Cell Companies (ICCs)**—as scale, jurisdictional reach, investor participation, and governance complexity expand.

Tokenization and Incentive Alignment

Accelerators issue **Accelerator Tokens (ATs)** to align incentives among startups, enterprises, investors, and individual contributors supplying resources or capital to bootstrap new ecosystems. Each Accelerator may raise funds through conventional financial instruments—such as **SAFE Notes**, **Convertible Notes**, or **Preferred Equity**—and may hold proceeds in conventional bank accounts or compliant **DeFi** equivalents. These proceeds are used to develop the shared infrastructure, resources, and tooling that enable **Exchange Networks**, **Resource Pools**, and **Quantum Privacy-enabled Solutions**.

Token minting and issuance are typically delegated to **Tokenization Service Providers**, ensuring consistency across jurisdictions and alignment with the broader **Quantum Privacy Exchange (QPX)** framework. This approach facilitates favorable deferred-tax and capital-gains treatment for participants under the fiscal architectures described in § **9**.

Accelerator Tokens (ATs) are distributed to founders, investors, teams, and partners as **attribution instruments** that capture the long-term value generated by the Accelerator's activities. Holders are entitled to proportional shares of revenues and derivative rights flowing from the **Exchange Networks** and **Resource Pools** seeded by the Accelerator, including allocations of **Exchange Tokens (EXCHs)**, **Resource Tokens (RTs)**, and **Resource Pool Tokens (RPTs)**. Distribution and entitlements are defined by each Accelerator's governing agreements, permitting flexible economics while remaining consistent with the unified governance and ownership principles of the Quantum Privacy Exchange (QPX).

To ensure that all tokenized rights and incentives remain verifiable, compliant, and lawfully enforceable across jurisdictions, each Accelerator operates within a network of **Quantum Privacy Cells (QPCs)** anchored by an **Accelerator Quantum Privacy Cell (AQPC)**. These

governance compartments provide the cryptographic, legal, and fiduciary foundations that bind every participant—individual, enterprise, or institution—to a unified, auditable framework of ownership, accountability, and incentive alignment, as described in the following section.

Accelerator Quantum Privacy Cells & Governance Interlinkage

Each **Quantum Privacy Accelerator ("Accelerator")** is bound to an **Accelerator Quantum Privacy Cell (AQPC)**, which serves as the **root governance compartment** of a network of **Quantum Privacy Cells (QPCs)** linking the individuals, enterprises, and institutions participating in that Accelerator. This architecture enables **privacy-preserving, decentralized coordination, contracting, and incentive alignment** across all participants.

Each **Accelerator QPC** is a **Manager-originated, deferred-activation compartment** created under **Quantum Privacy LLC** to confer **lawful recognition** of its members' resource contributions, participation rights, governance roles, and ownership interests. Unlike conventional identity or wallet constructs, **QPCs provide fiduciary and compliance standing** under applicable civil, commercial, and fiduciary law. They operate under confidentiality while maintaining **full auditability through the Unified Trust Model™ ledger**.

Through this structure, each QPC ensures that participating individuals and enterprises **retain ownership of their data, resources, and rights** while delegating operational authority to their **Personal or Enterprise Privacy Network (PPN/EPN)**. Compliance thereby becomes an **intrinsic property of system operation**, rather than an external or manual obligation.

Functionally, each Accelerator aggregates **verified contributions** from individuals, enterprises, governments, and institutions—transforming inputs such as **capital, data, infrastructure, expertise, trusted relationships, and intellectual property** into **tokenized, auditable rights** governed by the participants' respective QPCs or equivalent confidential entities.

Accelerators, Exchange Networks, and Resource Pools may each be associated with distinct **classes of Quantum Privacy Cells**, whose operating agreements define consistent frameworks for **governance, value sharing, dispute resolution, and compliance**. Collectively, these entities form a **legally and cryptographically interlinked governance fabric**—metaphorically *entangled*—through **cross-referenced operating agreements, shared verification protocols, and interoperable trust credentials**.

This **governance interlinkage and entanglement** enable decentralized coordination and verifiable trust among participants, even in the absence of direct contractual relationships

or prior affiliations. Through this adaptive structure, **Accelerators can self-organize, interconnect, and federate**, forming a **global lattice of interoperable, purpose-aligned networks** that continuously recycle verified value and accelerate lawful innovation at **near-zero marginal cost**.

6.3 Zero-Marginal-Cost Bootstrapping with Dual-Use Infrastructure

Both individuals and enterprises can leverage their existing legal, regulatory, and contractual rights and day-to-day activities to connect **dual-use resources**—assets, processes, or expenditures already embedded in existing operations—to the Exchange at **zero marginal cost**, using existing APIs, interfaces, and contractual frameworks. Because current infrastructure (e.g., IT systems, marketing budgets, data pipelines, or supply-chain integrations) can be reused without new capital expenditure, participants unlock value that was previously inaccessible due to regulatory or contractual friction.

This zero-marginal-cost reuse converts ordinary operational activities—such as customer engagement, regulatory reporting, or data exchange—into **tokenized contributions**, earning Exchange Tokens (EXCHs) or other tokenized rights without additional expense. Each dataset, model, workflow, or license agreement becomes a **reusable building block**, tracked through **Trust Blocks** and recorded as **Resource Tokens (RTs)** within the PNX.

Equivalent embodiments may employ encrypted databases, custodial trust registries, or zero-knowledge provenance systems that provide the same verifiable, privacy-preserving audit trail of lawful reuse.

By crowdsourcing participation, resources, and verified trust at scale, **Privacy Networks** form the **universal distribution and coordination layer** of the QPX and equivalent frameworks—anchoring system growth, amplifying liquidity, and ensuring equitable value-sharing among all lawful participants.

Through their integration with **Quantum Privacy Cells**, **Proof-of-Trust verification**, and **Unified Trust Model (UTM)** taxonomies, Quantum Privacy Networks establish the connective fabric that enables the PNX to function as a self-organizing, continuously auditable ecosystem—bridging people, enterprises, and institutions across every domain of human, digital, and ecological value.

7. Organizational Entities of the Quantum Privacy Exchange

The **Quantum Privacy Exchange (QPX)** operates as a **multi-layered architecture of legal, technical, and economic entities** that collectively enable **lawful, auditable, and privacy-preserving collaboration** among individuals, enterprises, and jurisdictions.

Each entity type—**Quantum Privacy Networks** (“Privacy Networks”), **Quantum Privacy Accelerators** (“Accelerators”), **Quantum Privacy Exchange Networks** (“Exchange

Networks"), and **Quantum Privacy Resource Pools** ("Resource Pools")—performs a **distinct yet interoperable function** within a unified framework of **trust, compliance, and verified accountability** governed by **Proof-of-Trust (PoT) attestations**.

All such entities may be **instantiated or anchored through Quantum Privacy Cells (QPCs)**, or functionally equivalent or similar **confidential limited-liability compartments**, which serve as the **foundational building blocks** of the Quantum Privacy Exchange ecosystem.

Together, these components create an **integrated, self-governing infrastructure** in which **compliance, privacy, and trust verification** are not external add-ons but **intrinsic properties of system operation**—embedding accountability directly into the fabric of modern digital and economic collaboration.

7.1 Personal and Enterprise Privacy Networks

Privacy Networks constitute the foundational participation layer of the PNX or any equivalent exchange infrastructure. They exist in two principal forms:

- **Personal Privacy Networks (PPNs)** unify an individual's applications, accounts, devices, messaging platforms, and digital assets into a secure, person-centered private network. They enable pseudonymous interaction, personalized services, and lawful value exchange with end-to-end privacy, security, compliance, and user control. Through EasyAccess™ consent mechanisms and Proof-of-Trust (PoT)–accredited Exchange Providers, individuals can enforce their legal and regulatory rights while safely contributing engagement, behavioral data, content, or other digital assets as Quantum Privacy Network Resources (QPN Resources). In return, participants may receive EasyAccess Reward Tokens (EARTs) for verified participation, Resource Tokens (RTs) for connecting validated resources to the Exchange, Exchange Tokens (EXCHs) for the incremental value those resources generate within the ecosystem, and Accelerator Tokens (ATs) for contributions to Quantum Privacy Accelerators and affiliated Exchange Networks.
- **Enterprise Privacy Networks (EPNs)** extend this model to organizations, enabling compliant and secure data collaboration, analytics, policy enforcement, and AI-driven automation across distributed systems and jurisdictions. Enterprises may contribute proprietary data, infrastructure, intellectual property, contractual rights, or other resources or assets as Resource Tokens (RTs) while maintaining full governance and control over compliance and usage. These resources can be aggregated into value-added Resource Derivatives or syndicated through Exchange Networks and Resource Pools, allowing proprietary or regulated assets to be pooled, monetized, and reused at zero marginal cost. In doing so, enterprises earn Exchange Tokens (EXCHs) for the value

generated within the Exchange, and Accelerator Tokens (ATs) when their contributions support or expand Quantum Privacy Accelerators and affiliated Exchange Networks, along with any associated derivative-rights allocations.

In practice, any PPNs or EPNs may simultaneously serve as **Solution Providers**, **Resource Providers**, or **Exchange Providers**, depending on context. They can independently participate in **Accelerators**, contribute to the formation of **Exchange Networks**, and pool resources into **Resource Pools**— as described in **Section 5 ("Organizational Entities of the Quantum Privacy Exchange")** and **Section 6 ("Treasury Layer and Token Platform")**, which together define the market, liquidity, and revenue-sharing mechanisms of the Quantum Privacy Exchange.

7.2 Quantum Privacy Exchange Networks

Quantum Privacy Exchange Networks ("Exchange Networks") function as **governed marketplaces** that define the **rules, trust criteria, and interoperability standards** for the trading, settlement, and redistribution of **tokenized resources**. Each Exchange Network operates as a **federated governance environment**, issuing **Exchange Tokens (EXCH)** that serve as the unit of **settlement, attribution, and participation rights** within the network. Participants earn tokens according to their **verified contributions** under the **Proof-of-Trust (PoT)** system.

Exchange Networks can **interconnect globally** through shared liquidity mechanisms and harmonized compliance standards, forming an **auditable web of interoperable markets** that bridge industries, jurisdictions, and regulatory regimes.

In a preferred embodiment, an **Exchange Network codifies its operating principles—rules, trust criteria, commercial terms, and interoperability standards—through Inter-QPC Agreements** (executed among the Quantum Privacy Cells of participating individuals, enterprises, or Accelerators), executable smart contracts, or functionally equivalent computable trust mechanisms. As summarized in § 3.8, **Inter-QPC Agreements enable privacy-preserving contractual enforcement by allowing obligations, conditions, and rights to be evaluated within the EasyAccess Authorization Network or inside each participant's Quantum Privacy Domain, without revealing proprietary, regulated, personal, or identifying information to counterparties or intermediaries.** This architecture allows Exchange Networks to function securely across institutions and jurisdictions that may not otherwise know or trust one another, while preserving strict privacy, cybersecurity, regulatory, and fiduciary compliance.

Building on these foundations, **Exchange Networks connect participating Personal and Enterprise Privacy Networks, each of which may act as a Quantum Privacy Solution Provider, Resource Provider, or Exchange Provider**. Coordination occurs through

tokenized agreements or computational contracts that govern how contributed resources are recombined, reprocessed, or syndicated into value-added Resource Derivatives.

By interfacing with **Quantum Privacy Resource Pools ("Resource Pools")**, Exchange Networks **establish the commercial terms, governance policies, and interoperability standards** necessary to support diverse, cross-domain markets within a unified framework of lawful trust and accountable data reuse.

Each Exchange Network **aggregates resources** from multiple providers, **transforms them into Resource Derivatives**—such as composites, augmentations, or computational outputs—and **organizes them into Resource Pools** with standardized governance and commercial frameworks. In addition, Exchange Networks provide essential services including **trust credentialing, interoperability, and policy enforcement**, enabling reliable cross-network collaboration and attribution. They may also **contract with Solution Providers or Enterprise Privacy Networks to grant rights to access or utilize specific Resources or Resource Pools** in exchange for payments, royalties, or fractional interests in Resource Derivatives.

Governance of Exchange Networks is anchored by the **Unified Trust Model (UTM)** and enforced through **Proof-of-Trust (PoT)**. While each network defines its own commercial and governance terms, an **Exchange Network itself may also be treated as a Quantum Privacy Resource**, represented by metadata and a Resource Token (RT), **enabling decentralized ownership, governance, and revenue sharing**.

Economically, Exchange Networks **allocate revenues and derivative rights** among participants in proportion to their verified contributions. Contributors earn **Exchange Tokens (EXCH)** when their resources are combined and utilized within the network. Holding EXCH entitles participants to **revenue shares, derivative value attribution, and governance input** over the network's rules and operations. EXCH may also be pooled across networks through **Exchange-level Liquidity Pools**, providing **liquidity, syndication, and reuse** across multiple domains.

In this way, **Exchange Networks serve as the market-structuring layer of the Quantum Privacy Exchange (QPX)**, transforming fragmented resources into standardized, value-added derivatives and coordinating their use across Resource and Liquidity Pools. Multiple Exchange Networks can operate in parallel across industries, geographies, and functions, scaling the QPX into a global framework for **resource pooling, reuse, and value creation**.

7.3 Quantum Privacy Resource Pools

Quantum Privacy Resource Pools ("**Resource Pools**" or "**Pools**") aggregate diverse tokenized assets — including **data, compute, content, models, intellectual property,**

and contractual rights — into standardized collections governed by uniform commercial, compliance, and provenance rules.

Each Pool issues **Resource Pool Tokens (RPTs)** that confer **proportional ownership, economic participation, and governance rights**. By pooling and tokenizing resources, the **Privacy Network Exchange (PNX)** enables participants to unlock **latent economic value** from underutilized infrastructure, knowledge, and digital assets — creating liquidity and compounding efficiency across the broader **Quantum Privacy Exchange (QPX)** ecosystem.

Resource Pools are **standardized groupings of Resource Tokens (RTs), Exchange Tokens (EXCH), and Resource Derivatives** that share **common governance, commercial terms, and semantic frameworks**. They provide a structured mechanism for **pooling, reusing, and syndicating resources at scale**, enabling efficient **valuation, rights management, securitization, and liquidity** across interoperable markets.

Each Pool aggregates heterogeneous resources — such as datasets, compute units, contractual rights, or engagement tokens — into **thematically aligned baskets** that may be accessed by **Solution Providers** under standardized terms with **verifiable semantics and provenance** encoded in **Trust Credentials**. This structure simplifies access to diverse resources, reduces negotiation complexity, and increases utility across domains such as **healthcare, finance, logistics, and AI training**. It also allows Resource Providers to **diversify risk, expand market access, and amplify revenues**, while ensuring **attribution and revenue distribution** flow back to contributors according to agreed-upon terms.

Governance of Resource Pools is enforced through the **Unified Trust Model (UTM)** and **Proof-of-Trust (PoT)**, which ensure that pooled resources meet consistent trust, provenance, and semantic requirements. Where **multiple QPCs jointly contribute, manage, or rely on a Resource Pool, the commercial terms, joint-use rights, and pooled-governance obligations may be formalized through Inter-QPC Agreements** (see § 3.8 and § 7.2), enabling privacy-preserving contractual coordination across participants without exposing proprietary, regulated, or personal information. **Pools may also be registered as QPX Resources** (or equivalently, PNX Resources) in their own right, represented by metadata and a Resource Pool Token (RPT) that denotes pro-rata ownership or participation rights in the pool. **This allows Resource Pools themselves to be referenced, syndicated, or traded as discrete assets**.

Economically, **RPT holders receive fractional revenue rights** generated from utilization of the pool's resources, creating ongoing **attribution and annuity-like value flows**. Pools may be established by **Exchange Networks, Accelerators, or individual Personal or Enterprise Privacy Networks (PPNs/EPNs)**, and may be instantiated through **Quantum Privacy Cells (QPCs)** to support specific markets or solutions. Because they interoperate

seamlessly across networks, Resource Pools are **foundational to scaling liquidity, reuse, and verified trust** within the PNX.

In essence, **Resource Pools function as the aggregation layer of the Quantum Privacy Exchange**, transforming fragmented contributions into **standardized, reusable bundles** that drive **sustainable market growth, deeper liquidity, and efficient participation** for both contributors and consumers.

7.4 Quantum Privacy Cells (Common Foundation of All Entities)

Confidential limited-liability compartments (such as Quantum Privacy Cells or functionally equivalent entities) serve as the atomic building blocks of the Quantum Privacy Exchange or any analogous lawful exchange architecture.

They provide the legal, operational, and cryptographic foundation for all higher-order entities—PPNs, EPNs, Accelerators, Exchange Networks, and Resource Pools.

Each Quantum Privacy Cell operates as a **privacy-native, deferred-activation governance compartment**. It automates contract execution, compliance verification, and benefit allocation across jurisdictions, allowing lawful collaboration among parties that may not know or trust one another.

By embedding compliance, policy enforcement, and auditability directly into their architecture, Quantum Privacy Cells make it possible to achieve **frictionless resource pooling, end-to-end process automation, and lawful global collaboration**—all while preserving privacy and eliminating the need for centralized intermediaries.

Through Quantum Privacy Cells, the Quantum Privacy Exchange becomes a **universal, person-centered economic fabric**, capable of supporting lawful, auditable value creation across every domain of human and institutional activity.

In preferred embodiments, these functions are implemented using the Quantum Privacy™, Proof-of-Trust™, Unified Trust Model™, and Quantum Privacy Exchange™ infrastructures developed by WebShield, Inc. In alternative embodiments, functionally equivalent systems employing distributed-ledger frameworks, regulated custodians, or other verifiable compliance and liquidity mechanisms may be used to achieve substantially the same results. Equivalent embodiments may substitute other confidential-governance frameworks, including smart-contract–based registries or regulated custodian networks, provided they achieve deferred activation, lawful auditability, and privacy-preserving governance.

8. Quantum Privacy Treasury Layer and Token Platform

The Quantum Privacy Treasury Layer and Token Platform form the financial foundation of the Quantum Privacy Accelerator and Exchange ecosystem described in **Sections 4 through 7**.

Where the organizational and governance structures enable lawful participation, verified contribution, and privacy-preserving collaboration, **the Treasury Layer provides the mechanisms that sustain liquidity, capitalization, and economic equilibrium across the network**. It operationalizes the principles of the Unified Trust Model (UTM) and Proof-of-Trust (PoT) by embedding compliance, auditability, and market efficiency directly into tokenized settlement and value distribution.

Through programmable liquidity, standardized treasury operations, and lawful securitization of verified rights, this layer converts verified participation and contribution records into a stable, tradable, and auditable medium of exchange—linking individual, institutional, and governmental participants into a continuous, self-funding global economy.

At the operational level, Liquidity Pools implement these treasury principles through compliance-verified mechanisms that stabilize value, balance inflows and outflows, and maintain continuous exchange among all verified participants and networks.

8.1 Quantum Privacy Liquidity Pools and Market Stabilization

Liquidity Pools—whether implemented directly within the Quantum Privacy Exchange as Quantum Privacy Liquidity Pools or via equivalent compliance-verified liquidity mechanisms—serve as the treasury, settlement, and stabilization layer of the exchange infrastructure. They provide a unified mechanism for managing inflows and outflows, supporting exchange, pricing, and collateralization of resources across the ecosystem.

By converting fiat, stablecoins, or tokenized assets into Exchange Tokens (EXCH) or equivalent settlement instruments under standardized allocation rules, **Liquidity Pools enable continuous market liquidity without requiring public listings or speculative trading**.

They also form the structural basis for deferred capital-gains treatment, allowing participants to hedge, borrow, or finance activities against verified token holdings while maintaining lawful compliance and verifiable provenance.

Benefits to Token Holders

For participants, Liquidity Pools provide the ability to buy, sell, hedge, or borrow against tokenized interests (e.g., QPX or equivalent tokens) while generally deferring taxation until redemption into fiat.

Tokens are structured to **accrue value over time** rather than distribute periodic income, thereby **avoiding phantom-income recognition** as long as beneficial ownership remains unchanged. This design **positions tokens for treatment as capital assets, with gains recognized only upon sale, redemption, or transfer—often eligible for long-term capital-gains rates if held for more than one year**. Participants thus gain liquidity, collateralization, and financing capacity without losing underlying ownership or governance rights, subject to the specific terms of each lending, staking, or derivative arrangement.

Benefits to the Exchange and Network Efficiency

At the system level, Liquidity Pools strengthen the efficiency, transparency, and resilience of the Quantum Privacy Exchange by **enabling accurate price discovery, verifiable value metrics, and continuous liquidity for assets that are complex, privacy-sensitive, long-duration, or that create societal value in addition to private profit**—such as healthcare outcomes, human capital, scientific research, and nature-based resources.

By aggregating tokenized claims from multiple Exchange Networks and Resource Pools, the QP Treasury Layer allows markets to **establish forward-looking valuations, diversify idiosyncratic risks, and enhance systemic liquidity** and stability across the ecosystem.

This architecture converts latent, illiquid, or under-recognized rights into verifiable, exchangeable value—**bridging private-sector innovation, public resources, and real-world social and economic outcomes** within a unified, compliance-verified market infrastructure.

8.2 Securitization and Market Formation

Liquidity Pools also enable the **securitization of tokenized assets**, creating institutional-grade markets for new categories of value. Tokens that represent perpetual annuities, deferred entitlements, or composite derivatives can be standardized and bundled into **bond-like instruments** or collateralized baskets, enabling investors to participate in long-term innovation and outcome-linked markets without direct operational exposure.

This securitization capability reduces the cost of capital, attracts institutional liquidity, and channels investment into ecosystems that depend on cross-organizational cooperation and deferred outcomes.

Through these mechanisms, **the Treasury Layer transforms tokenized participation rights into tradable, yield-bearing, or collateralizable instruments**—supporting continuous capitalization, transparent risk management, and efficient value recycling across the global Quantum Privacy Exchange.

8.3 Preferred Distributed Ledger Tokenization Layer (Hedera or Equivalent)

In a preferred embodiment, the QP Treasury Layer may be implemented on **Hedera Hashgraph**, or any equivalent compliance-grade distributed ledger providing native tokenization, consensus, and governance functions.

Hedera's **Token Service (HTS)** enables both fungible and non-fungible token issuance with programmable fee distribution, while its **Consensus Service (HCS)** provides immutable audit trails, regulatory guardrails, and verifiable sequencing of events. The **Hedera Governing Council**—comprising leading global enterprises, universities, and public-interest organizations—offers a tested model for decentralized yet institutionally credible governance.

These capabilities collectively enable the Quantum Privacy Token Platform to meet the highest standards of compliance, security, and operational assurance.

8.4 Equivalent Implementations and Alternative Frameworks

Equivalent embodiments may utilize **regulated custodian networks, federated treasuries, cooperative liquidity consortia, or jurisdiction-specific financial infrastructures** that perform substantially the same functions as the Quantum Privacy Treasury Layer. These alternative implementations may rely on national digital-asset platforms, multilateral settlement systems, private custodial registries, or institutional delegation frameworks—provided they support continuous liquidity, cryptographically verifiable provenance, and compliance-grade auditing, reporting, and asset segregation.

Such embodiments extend the Treasury Layer to jurisdictions or sectors where distributed-ledger infrastructure is limited or unavailable, ensuring universal applicability, backward compatibility, and interoperability with both public and private financial systems, including fiat custodians, regulated payment networks, and institutional registries.

Summary

Quantum Privacy Liquidity Pools—and equivalent Treasury mechanisms—form an **institutional-grade financial foundation** for the Quantum Privacy Exchange. By securitizing and collateralizing tokenized rights against real-world assets, the Treasury Layer bridges decentralized token economics with traditional capital-market structures, stabilizing liquidity, reducing capital costs, and enabling tax-efficient accrual of value. Through these mechanisms, the invention transforms privacy-preserving digital participation into a compliant, capital-efficient financial ecosystem capable of sustaining lawful global innovation at effectively zero marginal cost.

9.0 Quantum Rating Metrics & Schemes

The invention provides a comprehensive, privacy-preserving framework for generating, maintaining, and applying quantitative rating metrics ("Quantum Ratings") across the

Quantum Privacy Exchange (QPX). Unlike traditional rating systems—which rely on centralized data aggregation, unverifiable self-attestation, or manual audit—the Quantum Rating system leverages **Quantum Privacy**, **Proof-of-Trust (PoT)**, and the **Unified Trust Model (UTM)** to produce verifiable, high-resolution metrics at global scale without revealing personal, proprietary, or regulated data.

Under the Unified Trust Model, all participants, Resources, Resource Pools, and Exchange Networks are represented through **Trust Blocks** that encode identity proofs, provenance, semantic descriptors, compliance evidence, usage histories, and relationship lineages. These Trust Blocks link into a global **Privacy Graph**, allowing Quantum Ratings to evaluate the entire cryptographically verified lineage and provenance of any asset, participant, or computational output **without exposing underlying records**.

Because all computations occur within **Privacy Domains**—privacy-preserving execution environments governed by Quantum Privacy Cells (QPCs)—rating engines can compute many diverse rating schemes in parallel, all derived from the same underlying Trust Blocks and Privacy Graph. A single set of cryptographically sealed proofs can be recombined, weighted, and interpreted to produce dozens or hundreds of quantitative dimensions with extreme computational efficiency and low latency, enabling real-time market formation, solution orchestration, and cross-domain optimization.

This architecture allows for **fine-grained, evidence-based allocation of value** across Inter-QPC Agreements, Resource Pools, and Exchange Networks. Rewards, routing priority, token issuance, liquidity weighting, and revenue attribution can all be driven by quantitative metrics that reflect **verified contributions, verified provenance, and verified compliance**—not proxies, guesswork, or unverifiable claims. All Quantum Ratings are auditable and independently verifiable by regulators, fiduciaries, and neutral authorities. The full lineage of each metric is preserved as privacy-preserving proofs rooted in PoT attestations, ensuring fairness, accuracy, and resistance to manipulation.

Trust Taxonomies and Rating Classification Under the UTM

The Unified Trust Model (UTM) includes a **Trust Taxonomy Framework** that provides structured, semantically consistent classification of all Resources, participants, and organizational entities across the QPX ecosystem. This taxonomy defines:

- **Resource Classes** (e.g., data assets, compute assets, models, algorithms, IP, contractual rights, infrastructure, human expertise)
- **Trust Attributes** (e.g., provenance, quality benchmarks, regulatory applicability, risk category, semantic domain, dependency chains)
- **Operational Capabilities** (e.g., permitted computations, access rights, governance role, interoperability profile)

- **Jurisdictional Context** (e.g., GDPR-regulated, HIPAA-regulated, export-controlled, open-data, proprietary commercial asset)
- **Contribution Types** (e.g., technical, educational, governance, compliance, public-benefit, network-expansion)

These Trust Taxonomies establish **how disparate Resources and participants are indexed, compared, and mapped into Quantum Rating Schemes**, ensuring:

1. **Accurate Cross-Domain Comparability:** Rating engines can evaluate Resources that originate in different industries, jurisdictions, or regulatory regimes using standardized semantic categories. Example: A HIPAA-regulated health dataset and a proprietary financial model can both be compared under Compliance, Trust, Network Leverage, and Value Amplification Ratings with unambiguous consistency.
2. **Consistent Mapping Into Rating Dimensions:** Trust Taxonomy assignments determine which Trust Credentials feed into which Quantum Rating metrics—supporting deterministic, reproducible computation of metrics across markets and contexts. **Examples:**
   - A Resource classified as *Regulated Healthcare Data* maps directly into sector-specific compliance criteria, provenance checks, and safety requirements.
   - A participant classified as *Technical Contributor* feeds into Impact Contribution and Network Leverage ratings differently than a *Governance Contributor*.
3. **Semantic Alignment Across Jurisdictions & Markets:** Taxonomies ensure that rating engines interpret Resources and contributions consistently in multi-jurisdiction or cross-market scenarios, producing comparable metrics even when underlying legal requirements differ.
4. **Stable Input for Optimization, Governance, and Market Formation:** Because Trust Taxonomies explicitly define how Resources are interpreted in rating schemes, the Privacy-Preserving Process Optimization Service (PPOS), Treasury Layer logic, Exchange Networks, and AGPW policy systems receive consistent, semantically aligned inputs—eliminating ambiguity, drift, and fragmentation.
5. **Universal, Privacy-Preserving Classification:** All taxonomy assignments and rating mappings occur **inside Privacy Domains**, so no private, proprietary, or regulated data is disclosed, even though the classification logic operates globally across billions of Trust Blocks.

Together, these capabilities provide a universal mechanism for measuring, verifying, and rewarding value creation across the entire Privacy Network Exchange. Traditional

governance, economic, and social-benefit systems have long been constrained by the maxim:

"You can't improve what you can't measure—and you can't reward what you can't verify."

Quantum Ratings overcome this limitation. They allow the QPX ecosystem to:

- **measure outcomes without surveillance**,
- **reward contributions without disclosure**,
- **enforce fairness without centralization**, and
- **optimize markets, governance, and public-benefit flows under strict privacy guarantees**.

The combination of UTM Trust Taxonomies and Quantum Rating Schemes establishes a globally interoperable, privacy-preserving foundation for accurate measurement, equitable reward distribution, and trusted autonomy at scale.

9.1 Quantum Rating Dimensions Mapped Through UTM Trust Taxonomies

Under the Unified Trust Model (UTM), all participants, Resources, Resource Pools, and Exchange Networks are classified through **Trust Taxonomies**—structured semantic categories that describe provenance, regulatory status, operational capabilities, contribution types, and dependency relationships. These taxonomies determine **how Trust Credentials, PoT proofs, and Resource attributes map into each Quantum Rating Dimension**, ensuring consistent interpretation across jurisdictions, markets, industries, and technical domains.

Each Quantum Rating Dimension is thus computed not only from raw Trust Blocks and Privacy Graph metadata, but also from the **taxonomy-defined meaning** of the entity being rated. This ensures that all ratings are:

- semantically consistent across disparate Resource types,
- jurisdictionally aligned,
- interoperable across Exchange Networks and Resource Pools, and
- comparable across organizational and technological boundaries.

The canonical Quantum Rating Dimensions—augmented with explicit Trust Taxonomy integration—are as follows:

- **Trust Rating:** Measures the strength, authenticity, and completeness of Trust Credentials—including identity proofs, licensure, accreditation, authorship,

institutional affiliations, historical performance, and PoT-verified relationships—as classified under the UTM Trust Taxonomy.

Taxonomy categories determine which credentials are relevant (e.g., *Licensed Practitioner*, *Regulated Data Custodian*, *Accredited Expert*, *Enterprise Provider*) and how their Trust Blocks contribute to the overall Trust Rating.

- **Compliance Rating:** Quantifies adherence to the statutory, regulatory, contractual, and interoperability obligations defined in the UTM Trust Taxonomies for the Resource or participant category involved.

  Sector-specific taxonomy labels—such as *HIPAA-Regulated Data*, *GDPR-Controller*, *FERPA-Protected Record*, *Critical Infrastructure Provider*—govern which compliance criteria, risk models, and Trust Credentials are evaluated.

- **Data Quality & Provenance Rating:** Assesses integrity, utility, semantic structure, and PoT-verified lineage of contributed Resources according to their **taxonomy-defined class** (e.g., *Dataset*, *Model*, *Algorithm*, *Contract Right*, *Compute Asset*).

  The taxonomy determines which provenance benchmarks apply (e.g., update frequency, schema clarity, accuracy benchmarks, interoperability requirements) and how quality signals are weighted.

- **Safety & Adversarial Integrity Rating:** Evaluates resilience to adversarial misuse, unsafe behaviors, systemic vulnerabilities, and misalignment risks, using telemetry from QPASH, AGPW, and PoT-verified behavioral histories.

  The Trust Taxonomy dictates the applicable safety standards—e.g., *AI Model*, *Decision Support System*, *Regulated Workflow*, *High-Risk Infrastructure*—and routes each category to the correct safety and hazard-evaluation frameworks.

- **Impact Contribution Rating:** Measures cumulative, verifiable contributions based on taxonomy-defined contribution roles—*Technical Contributor*, *Governance Contributor*, *Network Expander*, *Educator*, *Solution Architect*, *Public-Benefit Actor*.

  Contribution types draw explicitly from the taxonomy's **Contribution Type** categories, aligning each record with the correct scoring model.

- **Network Leverage Rating:** Quantifies cross-domain value amplification based on the Resource's or participant's **taxonomy-defined interoperability profile**, composability attributes, and dependency relationships.

  For example, a Resource classified as a *Cross-Market Enabler* or an Enterprise tagged as a *Multi-Domain Participant* unlocks broader combinatorial leverage than one confined to a single sector.

- **Value Amplification Rating:** Measures incremental economic or operational value generated when taxonomy-compatible participants or Resources enter Inter-QPC Agreements that enable lawful augmentation, co-production, or syndication.

  Trust Taxonomies determine which combinations are legally, technically, or semantically interoperable—and therefore eligible for amplification scoring.

- **Systemic Risk & Resilience Rating:** Evaluates how a participant or Resource affects network-level concentration risk, dependency patterns, fault tolerance, and ecosystem resilience.

  Taxonomy-defined **Risk Classes** (e.g., *Critical Node*, *Redundant Provider*, *High-Dependency Asset*, *Low-Risk Contributor*) determine which metrics apply and how resilience scores are computed.

- **Public-Benefit Alignment Rating:** Quantifies contributions to societal goals—health, sustainability, education, safety, equity—based on taxonomy-defined **Public-Benefit Domains** (e.g., *Environmental Resource*, *Health Outcome Contributor*, *Civic-Transparency Enabler*).

  Taxonomies determine which public-benefit metrics are relevant to each Resource or participant type and how they feed into PBDR allocation and governance weighting.

Role of Trust Taxonomies in Rating Consistency & Cross-Domain Comparability

By embedding Trust Taxonomies into the computation of every Quantum Rating Dimension, the QPX ensures that:

- **identical actions produce identical rating impacts globally**, regardless of jurisdiction or sector;
- **different Resource types are evaluated under appropriate criteria**, not one-size-fits-all models;
- **Exchange Networks, Accelerators, and Resource Pools share a common semantic foundation** for routing, pricing, risk modeling, and optimization;
- **rating engines can operate efficiently on billions of Trust Blocks** without ambiguity or manual normalization; and
- **regulators and fiduciaries can independently verify rating lineage**, since all taxonomy mappings are encoded as PoT-verifiable Trust Blocks.

Together, these features make Trust Taxonomies a fundamental component of the Quantum Rating system—ensuring accuracy, fairness, interpretability, and cross-market coherence across the global Privacy Network Exchange.

9.2 Canonical Quantum Rating Dimensions (Taxonomy-Independent Definitions)

While rating schemes may evolve across jurisdictions, industries, or Exchange Networks, the invention defines several canonical dimensions that can be computed independently or combined into composite scores:

- **Trust Rating:** Measures the strength, authenticity, and completeness of Trust Credentials, including identity verification, licensure, accreditation, authorship, institutional affiliations, historical performance, and PoT-verified relationships. Trust Ratings influence routing, authorization, and risk-weighted allocation across Privacy Network Exchange markets.
- **Compliance Rating:** Quantifies adherence to statutory, regulatory, contractual, and interoperability obligations, including sector-specific requirements (e.g., HIPAA, GDPR, FERPA, GLBA), security policies, SLA commitments, and Exchange-level Trust Criteria. Compliance Ratings vary across jurisdictions and govern eligibility, routing priority, and allowable computation under Privacy Domains.
- **Data Quality & Provenance Rating:** Assesses the integrity, uniqueness, utility, semantic clarity, and PoT-verified provenance of contributed Resources—such as datasets, models, algorithms, infrastructure, or contractual rights. High scores reflect reliable lineage, consistent quality benchmarks, interoperability with Exchange Networks, and compliance-verified data-handling practices. This dimension supports PPOS optimization, risk reduction, and robust derivative-value formation.
- **Safety & Adversarial Integrity Rating:** Measures resistance to misuse, fraud, adversarial attacks, unsafe system behaviors, and harmful emergent dynamics. Derived from QPASH safety telemetry, anomaly detection, red-team analytics, AGPW trust coefficients, and PoT-verified behavioral patterns. High scores indicate strong alignment with safety guardrails, robustness under stress, and adherence to AI-safety guidelines across jurisdictions. This dimension ensures integrity, reliability, and resilience of participants, models, and workflows.
- **Impact Contribution Rating:** Measures cumulative, verifiable contributions—such as introductions, education, advocacy, onboarding, solution-building, standard-setting, and ecosystem-support activities (as enumerated under “Contribution Categories Recognized by Quantum Rating Schemes”). High Impact Contribution Ratings yield preferential routing, increased token yield, enhanced derivative rights, and greater visibility in PPOS-driven optimization.

- **Network Leverage Rating:** Quantifies the synergistic value a participant, Resource Pool, or Exchange Network adds when combined with others—capturing cross-domain complementarity, composability, and multiplicative network effects. High Network Leverage Ratings reflect the ability to increase system-wide efficiency, unlock latent derivative value, and improve matching outcomes across Exchange Networks and Liquidity Pools.
- **Value Amplification Rating:** Measures the incremental economic, optimization, or operational value produced when a participant or Resource Pool engages in an Inter-QPC Agreement or other tokenized collaboration. Captures co-production effects, privacy-preserving augmentation, cross-domain reuse, syndication outcomes, and measurable improvements validated through PPOS metrics and PoT attribution.
- **Systemic Risk & Resilience Rating:** Evaluates how a participant, Resource Pool, or Exchange Network affects network-level stability, concentration risk, correlated exposure, and resilience under stress. High scores indicate diversified relationships, redundancy in dependency chains, improved fault tolerance, and alignment with AGPW risk-balance guardrails. This dimension supports global ecosystem integrity and resilient market formation.
- **Public-Benefit Alignment Rating:** Quantifies contributions to measurable societal and public-benefit metrics—including health outcomes, sustainability, education, safety, civic transparency, and equity. Public-Benefit Alignment Ratings influence routing in PBDR-backed services, guide allocation of public-benefit derivative rights, and support lawful government participation under UTM/PoT.

First-Mover Advantage and Strategic Network Effects

Early and proactive participation in the Quantum Privacy Exchange materially strengthens these ratings for **both individuals and enterprises**. Individuals, investment firms, enterprises, solution vendors, and other participants that engage early—by evangelizing the network, onboarding Resources, forming Inter-QPC Agreements, assembling curated networks of complementary participants, or contributing to standards and interoperability—accumulate higher **Impact Contribution Ratings**, higher **Network Leverage Ratings**, and higher **Value Amplification Ratings**.

Importantly, an enterprise can benefit even **without a formal corporate decision** to become an early adopter: employees, customers, contractors, and ecosystem partners who participate through their own QPCs generate verifiable Contribution Records and network effects that elevate the enterprise's aggregated ratings. As these individual and organizational contributions compound across Inter-QPC Agreements and Exchange Networks, they create a durable, self-reinforcing strategic advantage relative to later adopters.

This advantage arises from two reinforcing mechanisms:

- **Natural Network-Effect Dynamics** — Because Exchange Networks, Resource Pools, and Inter-QPC Agreements create multiplicative value as additional participants integrate, early adopters capture outsized benefits from exponential network effects. Participants that assemble, curate, and grow their networks early enjoy greater derivative value, more efficient matching, and broader reach across the Privacy Network Exchange.
- **Deliberate Design Incentives** — The Quantum Privacy Rating System is engineered to reward early, constructive engagement. High-rating participants receive preferential routing, higher revenue yield, enhanced token allocation, and increased visibility within optimization workflows such as the Privacy-Preserving Process Optimization Service (PPOS). Firms that invest early in building high-quality networks, establishing interoperability, or catalyzing cross-domain collaboration accrue sustainable and growing advantages as the ecosystem scales.

Together, these mechanisms create a structural first-mover advantage: participants who adopt and curate their networks early—and whose QPCs contribute meaningfully to the growth, liquidity, or public-benefit performance of the ecosystem—establish a compounding lead that becomes progressively difficult for later entrants to match. This first-mover advantage is an intentional feature of the design, reinforcing the incentive-alignment architecture that accelerates lawful network formation and high-quality ecosystem expansion.

9.3 Contribution Categories Recognized by Quantum Rating Schemes

Quantum Rating Schemes rely on verifiable, privacy-preserving Contribution Records generated across the Quantum Privacy Exchange. The following categories represent common forms of measurable contribution by individuals, enterprises, institutions, or QPC-governed entities. These categories are illustrative and non-limiting:

- **Introductions & Network Expansion** — Verified introductions, endorsements, or referrals that bring new participants, enterprises, or Resource Providers into the ecosystem, including activation of new QPCs, Exchange Networks, or Resource Pools.
- **Engagement & Advocacy** — Educational outreach, ecosystem support, relationship development, and dissemination of EasyAccess-enabled content that increases lawful participation or awareness.
- **Technical & Intellectual Contributions** — Development, testing, auditing, or deployment of models, algorithms, clean-room processes, data pipelines, privacy-

preserving workflows, or solution components compatible with QPN, QPCs, UTM/PoT, or Exchange Networks.

- **Resource Contributions** — Provision or onboarding of data, compute, software, intellectual property, infrastructure, contractual rights, or other assets as Resource Tokens (RTs), Resource Derivatives, or Resource Pool components.
- **Commercial & Strategic Enablement** — Sourcing enterprise participants, forming pilots, establishing interoperability agreements, negotiating revenue-sharing arrangements, or providing business-development pathways that increase Exchange throughput or liquidity.
- **Solution Formation & Co-Development** — Building, integrating, or orchestrating solutions that leverage QPCs, Privacy Domains, ENs, or Resource Pools to produce measurable outcomes or improvements.
- **Governance, Compliance & Verification Participation** — Contributions to Trust Blocks, Trust Credentials, PoT verification processes, Inter-QPC governance agreements, or standards bodies for interoperability, compliance, and semantic alignment.
- **Public-Benefit Contributions** — Actions or Resource contributions that advance environmental, healthcare, educational, civic, sustainability, or other socially beneficial outcomes as recognized by public-benefit metrics evaluated within the QPX.

These illustrative categories allow Quantum Rating Schemes—including Impact Contribution Ratings—to quantify value creation consistently across Inter-QPC Agreements, Exchange Networks, Privacy Domains, and Accelerator ecosystems, while enabling future evolution of rating models and measurement frameworks.

9.4 Personalized and Context-Dependent Ratings

Quantum Ratings may vary based on:

- regulatory jurisdiction
- industry or domain (healthcare, finance, education, sustainability, logistics, AI)
- applicable Exchange Network or Resource Pool
- Trust Criteria governing specific participants or Resources
- the contracting purposes, relationships, or use case

A single participant or Resource may hold multiple contextually appropriate ratings simultaneously, enabling precise, risk-adjusted matching and efficient market allocation.

9.5 Generation of Diverse Quantum Rating Schemes

The invention supports parallel creation of diverse rating schemes derived from the same underlying Privacy Graph.

- Rating engines recombine Trust Credentials, PoT attestations, metadata, and verifiable events without duplicating data.
- Multiple schemes may coexist across markets, regulatory domains, or jurisdictions.
- All computations occur within Privacy Domains using zero-knowledge proofs or privacy-preserving aggregation.
- No personal, sensitive, or proprietary data is disclosed during rating generation.

Exchange Networks, regulators, enterprises, and Accelerators may define their own domain-specific schemes, enabling lawful diversity without undermining privacy, security, or compliance.

9.6 Application of Quantum Ratings in the Token Platform and PPOS

Quantum Ratings directly influence:

- token issuance, weighting, vesting, and redistribution (EXCH, RT, RPT, ATs, EARTs, QPTs)
- liquidity routing and settlement priority
- marketplace visibility, matching, and pricing
- derivative-rights allocation and revenue distribution
- contractual terms enforced through Inter-QPC Agreements
- PPOS process optimization, including stability, throughput, and fairness

Because ratings are derived from cryptographically verified events, the QPX allocates value transparently and efficiently while preserving strict privacy, fiduciary, and regulatory constraints.

9.7 Evolutionary and Adaptive Rating Mechanisms

Quantum Rating Schemes evolve dynamically over time based on:

- performance outcomes and historical effectiveness
- regulatory and jurisdictional changes
- feedback from domain-specific optimization engines
- governance updates within Exchange Networks
- changing needs of Resource Providers and Solution Providers
- global or jurisdictional public-benefit objectives

In advanced embodiments, AI systems—including LLMs and domain-specific machine-learning models—continuously analyze rating performance, predictive accuracy, and market efficiency to:

- propose new rating metrics or composite scoring dimensions;
- identify rating schemes that yield higher predictive value or better real-world outcomes;
- evolve rating models in response to ecosystem behavior;
- select among alternative rating formulations to optimize matching, liquidity, or societal benefit;
- auto-tune weighting functions to enhance fairness, stability, or economic efficiency.

These AI-augmented rating engines operate within Privacy Domains, ensuring that model training, evaluation, and adaptive updates occur without access to raw personal or proprietary data.

The result is a continuously improving, self-optimizing ecosystem in which Quantum Rating Schemes evolve based on measurable performance, enhancing allocation efficiency, market stability, equitable value distribution, and collectively beneficial outcomes across the Quantum Privacy Exchange.

10. Tax & Securitization Considerations

The Quantum Privacy Exchange (QPX) and its equivalent lawful frameworks establish an integrated legal, fiscal, and compliance architecture that ensures every verified transaction and allocation of value remains compliant, auditable, and economically efficient across jurisdictions.

By embedding fiscal transparency, deferred realization, and lawful securitization directly into the exchange infrastructure, the system enables participants to accumulate and exchange verified value under equitable, privacy-preserving conditions, without the need for centralized intermediaries.

10.1 Tax Treatment & Deferred Taxation Architecture

Although the preferred implementation employs the Quantum Privacy Token and Quantum Privacy Cell frameworks, equivalent embodiments may use any tokenization or rights-tracking mechanism that achieves substantially the same tax-efficient results—namely, pass-through treatment, elimination of entity-level tax, and deferred realization at capital-gains rates.

The QP Token and Quantum Privacy Cell architecture create a **globally extensible tax model that minimizes double taxation, eliminates corporate-level tax, and enables lawful deferral of income recognition until liquidity or realization events occur.**

In a preferred embodiment, **all Quantum Privacy ecosystem structures—including Personal Privacy Networks (PPNs), Enterprise Privacy Networks (EPNs), Accelerators, Exchange Networks, and, where applicable, Resource Pools—may be associated with and legally embodied through Quantum Privacy Cells (QPCs).** Each such structure also operates within a corresponding Privacy Domain, which provides a cryptographically bounded environment for privacy-preserving computation, contractual enforcement, liability ring-fencing, and tokenized rights management. The Privacy Domain further ensures that all accounting, attribution, and settlement computations occur within a cryptographically verifiable, privacy-preserving environment, supporting regulator-grade auditability without requiring disclosure of personal or proprietary data.

Together, the QPC and its Privacy Domain implement a unified legal-technical boundary that enforces Trust Criteria, governs access to regulated or proprietary data, enables execution of Inter-QPC Agreements, and provides a consistent mechanism for privacy-preserving attribution, settlement, and compliance across jurisdictions.

These QPCs may function as pass-through entities or non-entity coordination vehicles, including Series LLC cells, Cayman segregated portfolios, ADGM/DIFC protected cells, decentralized smart-contract pools, unincorporated DAOs, or equivalent contractual or on-chain governance frameworks. Each Quantum Privacy Cell functions as a flow-through compartment, ensuring that income, losses, and tokenized gains are allocated directly to participants in proportion to verified contributions rather than taxed at the entity level.

This architecture mirrors U.S. Subchapter K partnership treatment and analogous regimes under OECD, EU, and international frameworks, avoiding double taxation while maintaining compliance with jurisdiction-specific accounting and disclosure standards. Through modular design, Quantum Privacy Cells and Accelerators can interoperate across multiple tax regimes, adapting their flow-through logic to the requirements of local partnership, trust, or cooperative models.

Through modular design, Quantum Privacy Cells and Accelerators can interoperate across multiple tax regimes, adapting their flow-through logic to the requirements of local partnership, trust, or cooperative models.

Tax Treatment Design Considerations from prior WebShield filings—including, without limitation, the *Systems and Methods for Trust-Verified Tokenization & Settlement* provisional application filed October 7, 2025—are incorporated by reference, particularly

the privacy-preserving income-recognition and deferred-settlement mechanisms that harmonize compliance across the United States, European Union, Middle East, and Asia-Pacific territories.

Participants accrue tokenized value through Proof-of-Trust (PoT) verification events—for example, validated contributions, verified resource reuse, or authenticated performance milestones—but recognition of taxable income occurs only upon redemption, transfer, or other liquidity realization.

This structure allows verified tokenized rights to qualify for capital-gains treatment rather than ordinary income rates, aligning the tax profile of digital participation with the well-established treatment of long-term investment assets. To support international compliance, tokens or derivative rights may be distributed under either **streaming** or **accrual** modes:

- **Streaming mode** supports real-time micro-distributions in jurisdictions requiring immediate recognition and withholding.
- **Accrual mode** enables deferred reporting for participants eligible for capital-gains deferral or operating under tax-advantaged partnership models.

Because every lawful contribution—human, digital, or ecological—can generate verifiable, tokenized value, this architecture democratizes capital formation and wealth accumulation.

Traditional financial systems concentrate ownership among those with privileged access to capital and information. By contrast, the Quantum Privacy Exchange dynamically redistributes verified ownership and income through lawful, transparent participation—aligning economic rewards with measurable contribution, ethical behavior, and societal benefit.

Ultimately, this model extends the advantages of pass-through taxation, deferred realization, and equitable wealth accumulation to all lawful participants—individuals, enterprises, and governments alike—establishing a **person-centered global economy** in which verified contribution becomes a universal basis for value creation and exchange.

10.2 Securities Treatment and Lawful Securitization

QPX Tokens—including Exchange Tokens (EXCH), Resource Tokens (RTs), Accelerator Tokens (ATs), EasyAccess Reward Tokens (EARTs), Exchange Network Tokens (ENTs) and Exchange Root Tokens (ERTs)—are designed as **verified participation rights**, not speculative securities. Their value derives from measurable contributions, validated network effects, and lawful participation within governed ecosystems—not from passive expectation of profit through the entrepreneurial efforts of others.

Equivalent embodiments may express participation through **cooperative shares, membership interests, mutual-benefit certificates, or regulated asset tokens**, provided they maintain verified participation and compliance with applicable law. Each representation preserves the economic and governance rights of the contributor while avoiding classification as a security in most jurisdictions under principles similar to the U.S. Howey Test and EU MiCA frameworks.

At the same time, the system allows **selective securitization** to accommodate institutional capital and regulated investors. Verified pools of QPX Tokens, or their equivalents, may be aggregated and wrapped in compliant financial structures—such as **Regulation D, S, or A+** offerings in the United States, or equivalent regimes under Cayman, ADGM, DIFC, or EU directives—creating a lawful bridge between open participation and institutional finance.

This optional securitization enables pension funds, sovereign-wealth vehicles, and other regulated entities to invest in privacy-preserving ecosystems without violating fiduciary or prudential restrictions.

This hybrid model—**open participation combined with securities-grade compliance**—lowers the cost of capital, enhances liquidity, and aligns the innovation economy with global financial governance standards. Through embedded Proof-of-Trust verification and unified audit trails, tokenized instruments retain transparency, provenance, and compliance regardless of whether they circulate in decentralized or institutional contexts.

In effect, the Quantum Privacy Exchange architecture unifies **open-source participation with institutional finance**, enabling verified contributors and regulated investors to coexist within the same lawful market fabric.

This design bridges decentralized and traditional capital systems, transforming privacy, regulation, and fiduciary compliance from structural barriers into functional enablers of inclusive global prosperity.

10.3 Integrated Tax-and-Securities Compliance Framework

In preferred embodiments, the tax- and securities-treatment mechanisms described above are managed through a unified **Proof-of-Trust Compliance Service (PoT-CS)** that integrates regulatory credentialing, jurisdictional rules, and fiscal verification directly into token issuance and exchange logic. This service may:

- **Validate jurisdictional eligibility of participants and resources;**
- **Enforce withholding, distribution, and reporting requirements** through programmable policy logic; and

- **Generate cryptographically sealed Proofs of Compliance (PoC)** accessible to authorized tax or securities regulators.

This integrated compliance layer ensures that every transaction—whether a micro-distribution, liquidity-pool reallocation, or securitized issuance—remains consistent with applicable fiscal and securities laws while preserving participant privacy through zero-knowledge verification and consent-based disclosure.

11. Systemic Benefits & Global Impact

Democratized Participation and Liquidity

Through its **Accelerator**, **Exchange Network**, and **Resource Pool** structures, the Quantum Privacy Exchange (QPX) enables **universal access to finance, innovation, and ownership**.

Individuals and organizations can tokenize their verified contributions—capital, data, expertise, infrastructure, or intellectual property—into **liquid, tradable participation rights** that circulate lawfully across networks.

Liquidity Pools and **Treasury mechanisms** ensure that verified value flows efficiently and transparently, while **deferred-taxation frameworks** allow participants to accrue long-term wealth under equitable fiscal conditions.

Together with the **Universal Innovator Model** (Section 5), these mechanisms create a **self-funding economic engine** in which verified contribution—not pre-existing wealth or privilege—defines participation and reward.

By extending the benefits of liquidity, ownership, and capital formation to all lawful participants, the system transforms the global economy from **extractive and exclusive** to **inclusive and regenerative**—where every participant becomes both a **beneficiary** and a **steward** of collective prosperity.

Sustainability and Global Prosperity

At scale, the Quantum Privacy Exchange functions as an **adaptive coordination system** for sustainability and balanced growth. By enabling **verified, privacy-preserving optimization** of processes and resources (as described in Section 6), the network continuously improves efficiency while reducing environmental, regulatory, and ethical risk.

Economic value becomes linked to **measurable compliance, social benefit, and ecological stewardship**, creating new markets that reward positive externalities rather than exploit them. This integration of **trust, transparency, and tokenized economics** redefines the role of digital infrastructure in society.

It aligns **self-interest with public good**, **competition with cooperation**, and **innovation with responsibility**—producing a global system that grows **smarter, fairer, and more sustainable** over time.

By uniting privacy, governance, and market economics within a single adaptive architecture, the invention provides the **technical and legal foundation** for a more balanced world—one in which **innovation, accountability, and prosperity reinforce each other**.

The result is a **privacy-preserving trust economy** that delivers compounding benefits: higher productivity, equitable participation, sustainable growth, and greater human well-being.

In short, it establishes a system where **privacy, trust, and value creation** are not trade-offs but **inseparable dimensions of the same lawful, self-optimizing design**.

12. Recording, Verifying & Tokenizing Contributions

This section describes preferred embodiments for **documenting, classifying, verifying, and allocating rights associated with contributions by individuals and organizations that evangelize, design, develop, operate, and proliferate the Quantum Privacy Exchange (QPX) and Privacy-Network–enabled solutions**. The mechanisms below enable lawful, privacy-preserving attribution and reward across markets, geographies, platforms, and institutions, and support both embodiment-neutral claims and narrower claims that deter "plug-compatible" free-riding without licensing the Quantum Privacy IP portfolio or accepting PNX licensing terms.

12.1 Contribution & Engagement Recording System (CERS)

The **Contribution & Engagement Recording System (CERS)** operates as a governed service within an Accelerator, Exchange Network, or affiliated organizational domain, and comprises the following functional components:

1. **Contribution Capture Interfaces** — passive and active channels that accept contribution evidence such as email forwarding, tagged repository commits, structured web forms, encrypted uploads, and Enterprise Privacy Network (EPN) submission gateways.
2. **Classification & Tagging Layer** — a structured schema (the "Contribution Record") that normalizes engagement and resource types, milestones, counterparties, sector or market tags, and provenance to support automated analysis and equitable allocation.
3. **AI-Assisted Authoring & Evaluation** — prompt workflows, digital agents, and large-language-model summarizers that help Participants prepare accurate Contribution Records and assist Managers in assessing quality, impact, and relevance. These tools

may also autonomously generate draft records by linking and interpreting information gathered through the network of Contribution Capture Interfaces.

4. **Inferred Contribution Record Service** — a continuously operating analytics layer that aggregates, correlates, and analyzes data, communications, and recorded activities across multiple Participants and sources to identify and generate inferred or composite Contribution Records. Using pattern-recognition, graph-analysis, and semantic-linking methods, this service automatically attributes fractional participation to individuals, Series, or enterprises based on verifiable signals of involvement, collaboration, or influence. Inferred Records are cryptographically time-stamped, reviewed under Proof-of-Trust (PoT) verification, and—once validated—allocated or assigned to the appropriate Participants according to Unified Trust Model (UTM) policy logic.
5. **Proof-of-Trust (PoT) Verification** — cryptographic attestation services that bind Contribution Records (direct or inferred) to verifiable events, actors, and outcomes without revealing personal or proprietary information.
6. **UTM Taxonomy Mapping** — a semantic registry mapping both direct and inferred Contribution Records into Unified Trust Model taxonomies to ensure cross-network interoperability, transparency, and long-term comparability.
7. **Rights Allocation Engine** — a programmable policy layer that translates verified Contribution Records into fractional rights or tokenized interests (e.g., Accelerator Tokens), and, when applicable, into **Resource Tokens (RTs)** or **Resource Pool Tokens (RPTs)** associated with connected assets or outcomes.
8. **Tokenization & Routing Module** — an optional issuance and routing mechanism that generates, distributes, and records allocations of PNX token classes (AT, EXCH, RT, RPT, ENT, EART) to reflect verified value creation and maintain immutable audit-grade lineage.

12.2 Contribution Record (Data Model)

A Contribution Record is a structured, versioned object that captures:

- **Participant & Entity Linkage:** Participant identity (confidential), Series type (Individual/Enterprise/Accelerator/Affiliate), auto-generated Series ID, affiliations, keys/wallets, Trust Authority references, and verification status.
- **Commercial/Admin Preferences:** Participant-directed, Manager-administered, or hybrid administration; designated delegates/guardrails.
- **Engagement Milestones:** granular actions or events (e.g., introduction, amplification/endorsement, positive response, meeting scheduled/held, presentation/proposal/demo delivered, follow-on referrals, partnership strategy, EP3 Fellow/Affiliate recruiting, MOU signed, Series created, licensing/partnering executed, Accelerator/Exchange participation confirmed, enterprise customer added, resource

provider added, solution provider added, exchange provider added, financing term sheet drafted/committed/closed).

- **Classification Tags:** role, counterparty type/level, market focus, accelerator linkage, outcome status, verification method, timing, and impact metrics.
- **Evidence & Provenance:** linked messages, docs, commits, call notes, meeting artifacts; cryptographic hashes; time-stamps; Trust Blocks.
- **Updates & Continuity:** version history; superseding entries; Manager annotations.

12.3 Submission Channels (Preferred)

- **Passive Email** — Participants may copy or forward relevant emails to authorized Managers or the Executive Director. Including the phrase **"QPC Contribution Record – Submitted by [Name or Pseudonym]"** in the subject line or body constitutes a contemporaneous Contribution Record.
- **Repository Tagging** — Code or asset contributors may tag commits or pull requests with **"QPX Contribution Record – [QPC ID or Hash]"**, or link their GitHub/GitLab/PGP identity to their Quantum Privacy Cell via the Quantum Privacy Contribution Portal.
- **Private Uploads** — Encrypted web forms or secure drop-boxes may accept documents, URLs, commit hashes, AI-generated artifacts, or other materials supporting contribution verification.
- **Enterprise / EPN Submissions** — Enterprises, Accelerators, or affiliated organizations may submit Contribution Records on behalf of teams or individuals through Enterprise Privacy Network (EPN) nodes operating under delegated authority, with attribution assigned to the associated QPC(s).
- **AI-Assisted & Inferred Record Generation** — Authorized digital agents and analytic services operating within Privacy Domains or the EasyAccess Authorization Network may autonomously generate or suggest Contribution Records by aggregating verified communications, metadata, transcripts, or engagement logs. These records are (i) cryptographically time-stamped, (ii) validated under Proof-of-Trust (PoT), and (iii) subject to participant confirmation prior to allocation.

12.4 AI-Assisted Documentation & Evaluation

The AI-Assisted Documentation and Evaluation layer functions as an intelligent companion to the Contribution & Engagement Recording System (CERS). Large-language-model (LLM) prompts, digital agents, and autonomous analytic routines assist Participants in classifying activities, extracting contextual metadata, and drafting concise contribution narratives—in a preferred embodiment, aligned with the Exhibit-A taxonomy of the Quantum Privacy Cell Participation Agreement.

Evaluation agents—operating either under Manager supervision or pursuant to Manager-authorized governance policies—apply quantitative and qualitative scoring models to assess engagement quality, outcome likelihood, and network-level impact.

These systems may further interface with the Inferred Contribution Record Service (Section 5.2) to cross-validate direct and inferred activities, ensuring consistent attribution across Participants, Series, and organizations.

All generated or augmented Contribution Records remain provisional until verified and cryptographically sealed through the Proof-of-Trust (PoT) framework and incorporated into the Unified Trust Model (UTM) provenance ledger.

12.5 Automated Evaluation Metrics and Continuous Learning Loop

The Automated Evaluation Metrics and Continuous Learning Loop operates as a feedback subsystem within the AI-Assisted Documentation and Evaluation layer. It continuously refines the accuracy, fairness, and interpretability of engagement assessments by comparing predicted contribution scores and impact estimates against verified Proof-of-Trust (PoT) outcomes recorded in the Unified Trust Model (UTM) provenance ledger. Machine-learning models, statistical validators, and rule-based evaluators are periodically retrained using these verified results to improve the precision of classification, attribution, and valuation processes.

This adaptive calibration enables the Contribution & Engagement Recording System (CERS) to evolve dynamically with ecosystem scale—learning from real-world network behavior, regulatory changes, and evolving market conditions.

In preferred embodiments, the Continuous Learning Loop integrates differential-privacy safeguards and federated-learning architectures, allowing distributed Participants, Accelerators, and Enterprise Privacy Networks (EPNs) to contribute anonymized training data without exposing confidential or personally identifiable information.

Feedback metrics may include accuracy of attribution, timeliness of recognition, correlation with network-level value creation, and variance in inter-evaluator consistency.

Through this closed-loop mechanism, the system becomes progressively more effective at distinguishing high-impact contributions, minimizing bias, and ensuring equitable, auditable allocation of tokenized rights across the Quantum Privacy Exchange and affiliated Accelerators.

The result is a self-improving compliance and attribution fabric—one that transforms verified participation data into a continuously learning governance intelligence layer, enhancing both transparency and trust across distributed innovation ecosystems.

12.6 Proof-of-Trust Verification

Verification binds Contribution Records to cryptographic attestations without revealing sensitive content. PoT verifications may include:

- **Identity & Authority Proofs** (participant, enterprise signatory, or Trust Authority);
- **Event Confirmations** (meeting/calendar confirmations, signed MOUs, executed agreements, repository attestations);
- **Outcome Proofs** (pilot launched, integration complete, token allocation triggered, revenue recorded, partner onboarded, and improvement to metric or rating system).

Outcomes produce **Trust Blocks** or other equivalent verifiable records anchoring audit trails and enabling regulator-grade proofs while preserving confidentiality.

12.7 UTM Taxonomy Mapping (Interoperability)

Each Contribution Record is mapped into Unified Trust Model taxonomies (participant roles, market sectors, solution classes, governance attributes, resource types). This ensures:

- **Cross-network reuse** of evidence;
- **Comparability** across geographies/industries;
- **Stable semantics** for long-horizon analytics, valuation, and liquidity.

Mappings can be revised; lineage keeps prior semantics auditable.

12.8 Evaluation & Allocation Engine

Verified Contribution Records are processed against policy rules to propose and/or effect allocations, including:

- **Accelerator Tokens (ATs):** participation/attribution units tied to measured outcomes inside a domain Accelerator;
- **Exchange Tokens (EXCH):** when records contribute to exchange-level value creation;
- **EasyAccess Rewards (EART):** for consent/engagement-driven participation;
- **Governance/Network Tokens (ENT/PNT/ERT):** where governance participation or root exchange effects are verified;
- **Resource Tokens (RT) / Resource Pool Tokens (RPT):** when the contribution connects or creates assets (data/software/compute/content/IP/contract rights) usable by the Exchange.

Allocations may stream (micro-distributions) or accrue (deferred recognition), with jurisdiction-appropriate tax handling (see §7).

12.9 Mapping Contributions to Resource Tokens

When a Participant's action connects a **PN Resource** (dataset, model, workflow, software, compute, content, IP, contractual rights) to the Exchange, the system:

1. registers the asset via RT metadata (provenance, license/terms, permitted uses, trust constraints);
2. assigns fractional RT interests to appropriate Series per governing agreements;
3. (optionally) aggregates RTs into **RPTs** for standardized access/liquidity; and
4. links resulting derivative flows to AT/EXCH distributions as applicable.

This cleanly separates **engagement/evangelization value** (AT/EXCH/EART) from **asset-based value** (RT/RPT), while preserving full lineage.

12.10 Example Workflows (Illustrative)

A. Introduction → Positive Response → Meeting → MOU:
Passive email submission + calendar proof + MOU PDF → PoT verification → AT allocation; if an integration begins, EXCH accruals start; if a dataset connects, RT minted and mapped to RPT.

B. Code/Model Contribution via Repo:
Tagged commits + identity binding (PGP/Git handle ↔ Series) → PoT on merged PR → RT (software/model) issued; if adopted by an Exchange Network, associated EXCH and AT flows accrue under pool rules.

C. Enterprise Customer Added:
Executed license/SOW (uploaded) + EPN confirmation → PoT → EXCH issuance to contributors; if the enterprise contributes data/compute, RT/RPT minted to resource providers per commercial terms.

D. Resource Provider Onboarded:
Dual-use or PN-native asset connected through EasyAccess/API → RT/RPT issuance; Exchange Network terms define downstream EXCH distributions; contributors to onboarding receive AT/EXCH per policy.

12.11 Interoperability & Alternative Implementations

While a preferred embodiment uses Quantum Privacy Cells, the UTM, and PoT within PNX, functionally equivalent implementations may use:

- regulated custodial registries;
- smart-contract provenance with privacy layers;
- confidential computing for evaluation;
- cooperative/mutual governance forms.

Equivalence requires confidential recordkeeping, policy-verified attribution, audit-grade lineage, and rights allocation/routing substantially as described.

13. Privacy-Preserving Fiscal Compliance & Automated Financial Services

This section describes systems and methods that establish a lawful, privacy-preserving framework for financial reporting, taxation, and automated fiscal services within the Quantum Privacy Exchange (QPX) or any functionally equivalent infrastructure.

The invention extends the Quantum Privacy Cell and Unified Trust Model (UTM) architecture to fiscal governance, creating a unified compliance fabric that verifies income, assets, and obligations while maintaining cryptographic privacy.

Governance, Privacy, and Audit

All financial and governance records are maintained in encrypted privacy domains. Disclosures occur only through policy-authorized Trust Verification Requests validated under the UTM.

Manager-originated or Manager-recorded entries, when executed on a participant's behalf, carry the same evidentiary weight as participant-submitted records.

Audits replay cryptographically sealed Trust Blocks and lineage proofs, allowing complete traceability without revealing identities, trade secrets, or confidential financial details.

Versioning, Continuity, and Reconstitution

Financial and contribution records are versioned and amendable under continuous lineage control. When policy, regulatory, or personnel changes occur—or when a disclosure request or legal action arises—the system may automatically:

- freeze prior allocations and associated rights;
- reissue updated records under new policy parameters;
- reconstitute Series credentials to preserve lawful continuity; and
- maintain complete cryptographic provenance per the continuity methods of Claim Family 12.

In preferred embodiments, the continuity and reconstitution framework further includes dynamic substitution mechanisms that automatically detect and respond to trust-, reputation-, and performance-based changes among participants or resources. These triggers may include verified declines in compliance scores, trust-credential revocation, modification or addition of associated personnel, entities, or jurisdictions. Upon detection, the system may automatically freeze affected allocations, initiate substitution or reissuance of equivalent rights, and record cryptographically linked continuity proofs within the Unified Trust Model ledger. Such processes preserve lawful lineage and prevent

systemic disruption, ensuring that verified trust and value continuity are maintained even as participants, resources, or governance compositions evolve dynamically.

Anti-Gaming and Fraud Controls

Privacy-preserving graph analytics, duplicate-detection, and anomaly-scoring services continuously monitor for inflated, duplicative, or inconsistent financial claims. Detected anomalies are quarantined for Manager or automated review. Verified misrepresentations may trigger reclassification of affected allocations as Restricted Derivative Rights (RDR), with associated value redirected to Public-Benefit Derivative Rights (PBDR) pools.

Privacy-Preserving Fiscal Verification

Each Quantum Privacy Cell—or equivalent pass-through compartment—maintains verified records of income, gains, and asset values. Using cryptographic proofs generated under the UTM and validated through Proof-of-Trust (PoT) attestations, the system produces privacy-preserving proofs of income, asset value, and capital gains. Authorized fiscal gateways or accredited Trust Authorities may confirm conformity with applicable tax, tariff, and reporting obligations without access to underlying books or personal identifiers.

Automated Tax Filing and Remittance

Building on verified fiscal proofs, an Automated Tax Filing and Remittance Service compiles encrypted financial data, generates jurisdiction-specific filings, and executes real-time or periodic payments of taxes, tariffs, and fees.

Programmable policy logic embedded within Quantum Privacy Cells and Exchange-Network contracts performs continuous micro-withholding, jurisdictional allocation, and lawful settlement under audit-grade privacy guarantees. Regulators validate compliance through PoT attestations rather than direct access to source records.

Automated Financial Services and Liquidity Enablement

Verified fiscal proofs produced under this framework also support automated, low-cost financial services. Financial institutions—or algorithmic lending agents operating within PNX or equivalent systems—can evaluate creditworthiness and collateral sufficiency using privacy-preserving proofs of verified income, receivables, or Resource Pool interests. Tokenized representations of these assets may be pledged, traded, or securitized through Liquidity Pools to provide continuous, lawful liquidity without compromising compliance or confidentiality.

Outcome and Advantages

The disclosed systems establish a unified fiscal-governance architecture that:

- **eliminates entity-level taxation** through pass-through Quantum Privacy Cells;
- **enables deferred recognition and capital-gains treatment** where lawfully permitted;

- **automates compliance, remittance, and audit** through cryptographically protected, privacy-preserving computation within QPC Privacy Domains; and
- **expands equitable access to credit, insurance, liquidity, and verified participation benefits** for lawful contributors worldwide.

Collectively, these mechanisms convert fiscal administration from a manual, disclosure-dependent process into a self-executing, privacy-preserving trust fabric. They reduce administrative overhead, increase regulatory certainty, and align taxation, finance, and equitable participation—creating the technical and legal foundation for transparent yet confidential global economic engagement.

14. Privacy-Preserving Process Optimization Service (PPOS)

The **Privacy-Preserving Process Optimization Service (PPOS)** provides an intelligent orchestration and negotiation layer that continuously analyzes the resources, participants, and relationships within a distributed collaboration or exchange environment to identify optimal configurations for implementing, operating, and improving processes of any kind—including commercial, governmental, institutional, and personal workflows.

Operating within a **trust-verification and compliance framework** (such as, but not limited to, a Unified Trust Model or equivalent), the PPOS evaluates the complete ecosystem of participating entities, resource pools, exchange networks, and accelerator or innovation frameworks. It dynamically selects, negotiates, and recommends the most efficient, trustworthy, and compliant combinations of resources and participants for any given objective or policy constraint.

The PPOS functions at **any scale of operation**—from network-wide optimization across global collaboration frameworks, to sector- or geography-specific exchanges, to domain-specific resource pools, enterprise-level process orchestration, and even individual or family-level agents managing financial, operational, or sustainability-related activities.

At each layer, **autonomous process agents or equivalent intelligent components** act on behalf of their sponsoring organization, participant, or governance compartment, negotiating continuously with one another to improve performance, reduce waste, and align behavior with verified trust and compliance criteria. Together, these agents form a global market for efficiency and value optimization, where lawful, auditable interactions between digital agents progressively improve resource allocation, coordination, and measurable social and economic outcomes.

Each process element—whether a dataset, algorithm, organization, individual, or legal instrument—is associated with a **privacy-preserving trust credential** or equivalent verifiable record that encapsulates compliance status, jurisdictional constraints, quality

and performance metrics, and social or environmental attributes. The PPOS aggregates and analyzes these credentials to optimize workflows and resource selections while maintaining cryptographic confidentiality and auditability.

Optimization Criteria and Trust-Aware Parameters

The optimization engine incorporates multi-dimensional analytics and privacy-preserving computation to evaluate and balance:

- **Tax, Regulatory, and Compliance Burden:** dynamically models jurisdictional taxes, tariffs, and legal restrictions to minimize total cost while ensuring lawful compliance.
- **Environmental and Societal Impact:** evaluates sustainability, energy use, and social-equity factors to maximize positive impact and minimize harm.
- **Sanctions, Trade, and Jurisdictional Constraints:** identifies and excludes restricted entities or processes subject to sanctions or conflicting legal regimes.
- **Logistics, Cost, and Reliability:** accounts for infrastructure cost, availability, latency, and risk exposure to optimize quality of service and delivery efficiency.
- **Reputation, Ethics, and Integrity:** references verifiable trust attestations or equivalent ethical-standards frameworks to ensure that all participants meet requisite levels of integrity and fiduciary responsibility.
- **Relationship Graph and Incentive Compatibility:** uses a semantic or graph-based trust model to analyze collaboration history and incentive alignment, selecting configurations that enhance cooperation and systemic stability.
- **Governance and Public-Policy Alignment:** models how different configurations affect transparency, equity, and policy efficiency for governments, NGOs, or multilateral initiatives.
- **Personal and Family Optimization:** extends trust-based optimization to individuals and families, aligning financial, social, and environmental outcomes with personal values and verified ethical preferences.

Optimization Process and Operation

The PPOS continuously ingests encrypted telemetry, consented metadata, and verified trust or performance signals from participating systems, networks, and entities. Through distributed computation—employing **federated learning, secure multi-party computation, homomorphic encryption, or zero-knowledge optimization proofs**—the system computes **multi-objective optimization strategies** that satisfy both global and local trust constraints.

Autonomous process agents negotiate with each other in real time across organizational and jurisdictional boundaries. Using privacy-preserving negotiation protocols, these agents:

1. Propose or exchange optimized configurations based on their local trust, policy, and efficiency parameters;
2. Re-route workflows to higher-trust, lower-cost, or more sustainable providers;
3. Collaboratively balance workloads and incentives to achieve equitable, system-level outcomes; and
4. Generate **Proofs of Optimization** or equivalent attestations verifying the fairness, efficiency, and compliance of each negotiated configuration without revealing proprietary data.

Through these interactions, the PPOS evolves into a **distributed optimization marketplace**, where autonomous agents continuously trade and refine optimal configurations for data exchange, service orchestration, and resource reuse—converting complexity and regulatory diversity into measurable efficiency gains.

Integration with Verification and Governance Frameworks

All optimization events and resulting configurations are verified and immutably recorded through a **trust-verification and attestation framework**, which may include, but is not limited to, a Proof-of-Trust (PoT) process, or any equivalent system that ensures lawful auditability without disclosure of sensitive information.

Participating entities and their process agents may autonomously implement PPOS recommendations through **policy-governed logic, automated contract systems, or equivalent programmable frameworks**, creating self-optimizing governance structures that adapt in real time to changes in law, economics, or environmental conditions.

The PPOS may further issue **optimization tokens** or equivalent reward instruments to record and redistribute measurable value generated through verified efficiency or sustainability improvements. These tokens may interoperate with other digital-asset or value-exchange systems—such as participation tokens, exchange tokens, or resource-pool tokens—to ensure that the value of optimized coordination is transparently captured, verified, and shared across all lawful participants.

By embedding adaptive optimization intelligence and autonomous negotiation directly into distributed collaboration frameworks, the PPOS transforms complex multi-party systems into a **self-organizing, continuously improving global trust economy**.

Whether optimizing a multinational supply chain, a national healthcare program, an enterprise process, or a household's resource use, the PPOS converts legal, economic, and ethical constraints into dynamic collaboration opportunities.

Participants benefit from lower costs, improved compliance assurance, stronger environmental and social alignment, and greater resilience to market and regulatory change.

At global scale, these mechanisms enable a **universal market for lawful efficiency**—a network where verified trust and value flow seamlessly across individuals, enterprises, and governments.

The result is an economy that grows smarter, fairer, and more sustainable over time—one in which the pursuit of efficiency aligns naturally with societal well-being, equitable prosperity, and the flourishing of people and planet alike.

15. Tokenized Market Formation & Revenue-Sharing Architecture

The systems and methods described in this section build upon the contribution, verification, and tokenization frameworks introduced in **§ 6–8**—including the Accelerator and Exchange architectures, Quantum Resource Pools, and the Treasury and Liquidity mechanisms. Together, these elements enable a lawful, privacy-preserving marketplace in which verified contributions, resources, and relationships are converted into tokenized economic rights and exchanged through decentralized, compliance-verified networks.

The invention provides a generalizable model through which individuals, enterprises, and institutions may participate in global, self-funding markets that align incentives, amplify network effects, and equitably distribute verified value creation.

Structural Limitations of DAO-Based & Traditional Token Governance Models

Most distributed-ledger and DAO-based governance systems—despite meaningful advances in transparency, programmability, and decentralized coordination—cannot support lawful, regulated, or population-scale participation. Their limitations stand in sharp contrast to the capabilities of the Quantum Privacy Exchange (QPX), and help illustrate the systemic advantages of the present invention.

1. Public-Ledger Transparency Prevents Participation by Regulated Actors

DAO governance models inherently record voting histories, ownership graphs, participation events, and economic rights on transparent or semi-transparent ledgers. For regulated actors—including executives, employees, fiduciaries, consultants, investment managers, public officials, or academic researchers—this creates immediate legal conflicts. Public discoverability of contingent compensation, token holdings, or governance participation is enough to violate employment agreements, conflict-of-interest rules, fiduciary duties, professional-conduct standards, client-

confidentiality obligations, and anti-bribery statutes such as the FCPA, 18 U.S.C. § 201, the OECD Anti-Bribery Convention, and the U.K. Bribery Act.

As a result, most professionals who operate under regulatory or contractual constraints are legally barred from participating in DAO ecosystems—not because of intent, but because the architecture itself forces prohibited disclosure.

The QPX architecture resolves this through undiscoverable participation, deferred activation, encrypted provenance, and Proof-of-Trust (PoT) verification. Participants may lawfully contribute, collaborate, or accrue contingent rights without exposing confidential affiliations or creating discoverable inducements.

2. DAO Governance Cannot Enforce Fiduciary, Regulatory, or Contractual Prerequisites

Traditional DAO frameworks have no way to determine whether a participant is legally permitted to engage in a given activity. They cannot verify fiduciary status, employment restrictions, contractual obligations, or professional-ethics boundaries. Smart contracts cannot interpret jurisdiction-specific rules, evaluate conflicts of interest, enforce preconditions for eligibility, or prevent unauthorized inducements. Once a transaction executes, DAO systems also lack any mechanism to re-route restricted value to a compliant recipient or custodial pool.

The QPX resolves this structural gap through its integrated compliance fabric. Compliance Graphs, Trust Taxonomies within the Unified Trust Model (UTM), and PoT prerequisites ensure that no right or benefit becomes active until all fiduciary, contractual, ethical, and regulatory criteria have been satisfied. If a disqualification arises, the system adapts automatically—substituting a compliant participant or redirecting restricted value into Public-Benefit Derivative Rights (PBDR) pools with full cryptographic provenance. Governance becomes proactive, rule-verified, and legally enforceable rather than permissive and post-hoc.

3. DAOs Fragment Trust and Reduce Interoperability

Permissioned or private DAOs attempt to mitigate the visibility problems of public blockchains but introduce fragmentation instead. Each becomes a separate, incompatible trust domain with its own local semantics, credential formats, identity assumptions, and governance logic. Such systems cannot share provenance, compliance evidence, or meaningful lineage across organizational, jurisdictional, or technological boundaries. Cross-network collaboration requires either over-disclosure or fragile, unverifiable interoperability layers.

By contrast, the QPX leverages the Unified Trust Model, interoperable Trust Taxonomies, and a global Privacy Graph that encodes cryptographically verified lineage across participants, Resources, Resource Pools, and Exchange Networks. Trust becomes composable rather than siloed, enabling unified governance, liquidity, and market formation across enterprises, regulators, industries, and sovereign domains without sacrificing privacy or compliance.

4. DAO Token Models Cannot Deliver Lawful, Continuous, or Scalable Market Formation

DAO token models lack the architectural substrates required for lawful, population-scale markets. They have no reliable mechanism for establishing identity or eligibility at scale, cannot embed jurisdiction-specific trust criteria into token flows or liquidity operations, and cannot integrate with regulated institutions. They also lack deferred vesting, conditional activation, lawful redistribution, or continuity protections when a participant becomes disqualified.

The QPX remedies these structural deficiencies by integrating liquidity, tokenization, compliance, rights management, and Resource coordination into a unified, trust-verified economic fabric. Because each Quantum Privacy Cell (QPC), Resource Token, and Exchange Network operates under Trust Block lineage and PoT verification, token issuance, liquidity provisioning, securitization, revenue allocation, risk-weighted redistribution, and dynamic substitution can occur lawfully, continuously, and at global scale. Markets form adaptively and in real time under strict privacy, compliance, and provenance guarantees—capabilities no DAO or traditional token system can achieve.

Participant Roles and Dual-Use Resource Model

Any lawful person or organization may participate in the universal exchange architecture as a **Resource Provider**, **Exchange Provider**, and/or **Solution Provider**, individually or in combination, through the governance structure of a Quantum Privacy Cell or functionally equivalent limited-liability compartment.

Each participation agreement defines the initial terms for contribution, participation, and value sharing, while maintaining flexibility for deferred or conditional activation based on verified Proof-of-Trust (PoT) credentials as detailed in § 4.

Existing legal agreements and business relationships among participants may also be incorporated as dual-use resources. By mapping these legacy contracts into standardized metadata structures and attaching cryptographic trust credentials, the system bootstraps the Quantum Privacy Exchange (or equivalent ecosystem) from existing commercial, institutional, or governmental infrastructures without requiring their

replacement. This dual-use capability dramatically reduces friction in network launch and adoption.

Exchange Networks and Resource Pools

Exchange Networks interconnect Resource, Exchange, and Solution Providers through standardized, auditable agreements—whether implemented contractually or programmatically—that define trust criteria, usage rights, compensation, and revenue-allocation logic.

Each Exchange Network may represent a sector, geography, jurisdiction, joint venture, collaborative, or policy domain, or an equivalently defined collaboration context, while maintaining interoperability through shared trust credentials and token-class mappings.

Exchange Networks can interoperate horizontally and vertically, forming a multi-layered "network of networks" that enables both specialization and reuse. They may connect distinct industries, communities, or public-private collaboratives under a common trust fabric, allowing lawful resource reuse and service integration across previously isolated markets.

Resource Pools aggregate tokenized resources—such as datasets, algorithms, infrastructure components, intellectual property, or compliance proofs—making them discoverable and accessible for lawful reuse across multiple Exchange Networks. Each Resource Pool operates under policy-driven access rules verified through the Unified Trust Model (UTM) or an equivalent framework.

Liquidity Pools and Settlement Layer

Quantum Privacy Liquidity Pools provide continuous funding and settlement within and across Exchange Networks by automatically redistributing verified value derived from tokenized transactions, royalties, or usage fees. Each pool maintains proportional balances in one or more token classes and allocates liquidity according to verified PoT attestations and network-defined policies.

The settlement layer employs programmable compliance logic that ensures lawful jurisdictional allocation, revenue recognition, and tax withholding consistent with § 7.1 (Tax Treatment and Deferred Taxation Architecture). This design eliminates intermediaries while maintaining regulatory integrity and full auditability under cryptographic privacy guarantees.

Incentive Alignment and Value-Sharing Mechanisms

The revenue-sharing architecture disclosed herein enables proportional and auditable reward allocation to all verified participants who contribute to the creation, operation, or scaling of Exchange Networks, Resource Pools, or Accelerators.

Each verified contribution—whether intellectual, financial, operational, or relational—is logged as a Contribution Record under § 5 and converted into fractional economic rights represented by Accelerator Tokens (ATs), Exchange Tokens (EXCH), Resource Tokens (RTs), or Resource Pool Tokens (RPTs).

Revenue and value flows are programmatically routed according to predefined sharing logic, ensuring that all lawful contributors receive verified, traceable participation rewards. By tying token allocation to Proof-of-Trust events, the system enforces continuous alignment between verified behavior and realized economic benefit, transforming compliance from a cost center into a value-generation mechanism.

Marketplace Formation and Dynamic Terms of Exchange

During initial deployment, revenue-sharing terms and participation rights may be defined through contractual instruments such as Distribution Agreements or equivalent digital participation frameworks. Each such agreement defines the initial rules for engagement, contribution, and value sharing within a Quantum Privacy Cell, Accelerator, or equivalent legal compartment. Deferred Activation provisions allow participation rights to vest only upon verified compliance, enabling lawful network bootstrapping from zero initial capital or participants.

As the Exchange Network matures, these agreements transition to autonomous enforcement through programmatic Inter-QPC Agreements executed within the Privacy Domains of participating Quantum Privacy Cells, where pricing, allocation, and sharing terms adjust dynamically based on verified demand, trust ratings, and supply conditions.

In alternative embodiments, these same obligations may be implemented through smart-contract frameworks, decentralized coordination mechanisms, tokenized computational contracts, or other functionally equivalent on-chain or off-chain governance infrastructures that provide verifiable, automated enforcement. Existing agreements among participants may also be imported, wrapped, or synthesized as dual-use resources to accelerate network launch, interoperability, and cross-domain integration.

Accordingly, the invention provides a generalized mechanism by which any lawful network of participants can evolve from conventional contract-based collaboration to fully automated, tokenized exchange and settlement under cryptographic and fiduciary assurance.

Token Framework and Governance Mechanisms

The token architecture builds on the classification and governance frameworks introduced in §§ 6–8, which define how verified rights, revenues, and obligations are expressed through interoperable token classes. Within each Exchange Network, governance rules are enforced through **programmatic Inter-QPC Agreements executed inside the Privacy**

Domains of participating Quantum Privacy Cells, where token issuance, vesting, redistribution, and settlement occur through privacy-preserving, PoT-verified computation.

In alternative embodiments, these same mechanisms may be implemented through smart-contract frameworks, decentralized coordination services, or other functionally equivalent computational trust systems. Oversight may be provided by Accelerators, Trust Authorities, or other jurisdictionally recognized fiduciaries, ensuring that tokenized governance remains lawful, auditable, and cryptographically verifiable across jurisdictions.

Network Effects and Economic Amplification

By linking verified resources, liquidity, and governance under a shared compliance and attribution fabric, the system creates self-reinforcing positive network effects. Each new resource or participant increases the marginal utility of all existing participants by expanding the set of lawful, trust-verified relationships available for collaboration.

Dual-use resources—those already operating under conventional licenses, data-sharing frameworks, or commercial agreements—can be attached to the exchange infrastructure with minimal integration effort, accelerating adoption and value creation.

This architecture thus supports exponential network scaling and value amplification without compromising regulatory integrity or ethical accountability.

Outcome: Universal Infrastructure for Lawful Value Exchange

Through the mechanisms described above, the invention establishes a universal, compliance-verified exchange infrastructure that unifies contributions, resources, and markets into a single adaptive economic fabric. By embedding trust, liquidity, and incentive alignment directly into the system's architecture, participants across innovation ecosystems, corporations, governments, and civil society can collaborate efficiently, transparently, and lawfully. The result is a self-funding, privacy-preserving, and continuously optimizing economy in which verified trust replaces coercive control, and equitable participation replaces exclusion—driving sustainable growth, stronger institutions, and shared prosperity for individuals and societies alike.

Illustrative Claims (Non-Limiting)

Preamble and Disclaimer

The following illustrative claims are provided as part of this provisional application to further define and clarify the inventive concepts disclosed herein. These claims are **non-limiting** and are included to demonstrate representative embodiments, system

architectures, and method operations that may be practiced within the scope of the invention.

Although a provisional application is not required to contain formal claims, the Applicant expressly incorporates the following claim language into the disclosure so that each element, combination, and functional relationship described herein shall be deemed **constructively disclosed** as of this filing date under **35 U.S.C. § 119(e)** and **§ 120**. The illustrative claims therefore serve to:

1. Establish **priority** for the described subject matter, including the structures, processes, and inter-relationships among system and method components;
2. Provide **enablement and written-description support** under **35 U.S.C. § 112(a)** for future non-provisional, continuation, and continuation-in-part applications; and
3. Clarify the Applicant's possession of each disclosed embodiment and its variants, whether claimed herein or not.

The claims set forth below are **illustrative only** and should not be interpreted as limiting the scope of the invention to the specific combinations, steps, or components recited. Additional claims of broader or narrower scope may be presented in subsequent applications that rely upon the present disclosure for priority and enablement.

Each family group organizes related claims by functional architecture, operational process, and application domain, and maps their dependency to the Applicant's earlier filings. These earlier filings collectively establish the foundational inventions upon which the present claims build, and include the following applications, each of which is expressly incorporated herein by reference as set forth in the **CROSS-REFERENCE TO RELATED APPLICATIONS** section:

- **U.S. Patent No. 12,316,610 B1**, titled *"Privacy Network and Unified Trust Model"* (priority to 2016);
- **U.S. Patent Application No. 19/206,859**, filed May 13, 2025, titled *"Quantum Privacy, Proof of Trust, and Privacy Network Exchange,"* which is a Continuation-in-Part of U.S. Patent No. 12,316,610 B1;
- **U.S. Provisional Patent Application No. 63/804,583**, filed May 12, 2025, titled *"Quantum Privacy, Proof of Trust, and Privacy Network Exchange"*;
- **U.S. Provisional Patent Application No. 63/895,861**, filed October 7, 2025, titled *"Systems and Methods for Trust-Verified Tokenization & Settlement"*;

- **U.S. Provisional Patent Application No. 63/923,253**, filed November 22, 2025, titled *"Systems and Methods for Quantum Privacy-Enabled Self-Funding AI Trust, Safety & Compliance"*; and
- **U.S. Provisional Patent Application No. 63/926,629**, filed November 27, 2025, titled *"Systems and Methods for Quantum Privacy-Enabled Personalized, Value-Based Universal Exchange for Better Health."*

These applications collectively provide the statutory basis for priority, written description, and enablement for the present disclosure, and the illustrative claims set forth herein should be understood as refinements, extensions, and representative embodiments of the inventions described across this integrated family of filings.

GROUP 1 — QUANTUM PRIVACY CELLS & PRIVACY DOMAINS (Claims 1-37)

Quantum Privacy Cells (QPCs) serve as the foundational trust, identity, and computational boundary for all participants—human, enterprise, device, agent, or system—within the Quantum Privacy Network. A QPC represents the smallest enforceable privacy, provenance, and policy-governed unit of computation. Every QPC defines a sealed Privacy Domain that enforces cryptographically bounded lawful computation, meaning that all data access, model execution, agent behavior, and computational processes are governed by Trust Criteria, Proof-of-Trust lineage, and policy enforcement constraints. QPCs unify identity, provenance, consent, jurisdiction, contractual rights, and computation under a single cryptographic and policy-enforced boundary.

QPCs also provide the substrate for establishing verifiable relationships, forming Inter-QPC Agreements, enabling privacy-preserving computation, safeguarding private data, executing distributed workflows, and governing resource usage. This Group defines the core primitives used across the entire QPN/QPX architecture, enabling any vendor, enterprise, regulator, or infrastructure provider to participate securely while maintaining compliance across jurisdictions and sectors. QPC-based privacy governance represents a significant advance over legacy identity systems, enclave models, and decentralized architectures that lack enforceable trust and policy alignment.

Family 1.1 — Foundational QPC Architecture & Privacy Domains

Covers the definition, instantiation, and enforcement layer of Quantum Privacy Cells. It includes how QPCs establish privacy boundaries, unify identity and provenance, bind rights and obligations, enforce jurisdictional rules, control computation, and govern interactions with enterprises, applications, devices, and external systems. QPCs allow computation to occur without disclosing internal data, enforcing both data minimization and cryptographically verifiable lawful computation. Privacy Domains defined by QPCs

ensure that all code execution, AI inference, data transformation, and state changes honor Trust Criteria and Proof-of-Trust lineage while preserving strict confidentiality.

Applies to identity platforms, cloud providers, compliance engines, AI governance systems, healthcare networks, financial institutions, and all regulated data environments. Vendors receive an enforceable, audit-ready privacy primitive that eliminates the need for centralized data aggregation or insecure enclave-based designs. Provides the foundational layer of the CIP claim set and serves as the legal backbone for enforcement across every other Group and Family in the QPN ecosystem.

Claim 1. A system comprising, in any operable combination, one or more of:

- **(a)** a **Quantum Privacy Cell** (QPC) instantiated for a participant, device, enterprise, or agent, the QPC defining a cryptographically enforced Privacy Domain;
- **(b)** a **boundary-enforcement layer** restricting all computation to operations permitted under Trust Criteria;
- **(c)** a **provenance-governed identity substrate** binding participant, device, enterprise, or agent attributes to Trust Blocks;
- **(d)** a **jurisdiction-aware policy layer** constraining computation based on regulatory, contractual, or constitutional requirements; and
- **(e)** a **privacy-preserving interaction interface** mediating all communications between the QPC and external systems;

Wherein the system executes within a QPN-enabled infrastructure comprising at least one of: QPCs, Privacy Domains, Trust Criteria, Proof-of-Trust, Trust Blocks, or EasyAccess workflow threads.

Claim 2. The system of Claim 1 wherein **the Privacy Domain prevents leakage of personal, proprietary, or regulated data through runtime, computation, or model inference.**

Claim 3. The system of Claim 1 wherein **QPC instantiation occurs upon onboarding, identity verification, consent capture, or policy-enforced activation.**

Claim 4. The system of Claim 1 wherein **Trust Blocks encode lineage, provenance, consent, regulatory attributes, or rights assignments.**

Claim 5. The system of Claim 1 wherein **the Privacy Domain enforces cryptographically bounded lawful computation restricting all actions to approved Trust Criteria.**

Claim 6. The system of Claim 1 wherein **a QPC anchors identity across PPNs, EPNs, devices, applications, or systems.**

Claim 7. The system of Claim 1 wherein **the QPC includes cryptographic sealing of computation results to provide verifiable provenance.**

Claim 8. The system of Claim 1 wherein **Privacy Domain boundaries prevent unauthorized model access, training leakage, or AI inference inversion.**

Claim 9. The system of Claim 1 wherein **QPC activation includes allocation of policy weights, rights, obligations, and participant authority.**

Claim 10. The system of Claim 1 wherein **QPCs maintain a continuous state machine governed by Trust Criteria and Proof-of-Trust lineage.**

Claim 11. The system of Claim 1 wherein **multiple Privacy Domains coexist with enforced isolation to prevent unauthorized cross-domain access.**

Claim 12. The system of Claim 1 wherein **QPCs govern secure execution of AI agents within privacy-bounded compute environments.**

Claim 13. The system of Claim 1 wherein **QPCs enforce jurisdictional routing or computational constraints based on participant attributes.**

Claim 14. **A method comprising:**

(a) instantiating a QPC for a participant or system;
(b) defining a cryptographically bounded Privacy Domain;
(c) binding rights, obligations, or provenance attributes to Trust Blocks;
(d) enforcing Trust Criteria during computation; and
(e) mediating interactions through privacy-preserving interfaces;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Family 1.2 — QPC-Governed Execution, Boundary Control & Lawful Computation

Covers how QPCs govern and constrain all forms of computation or interaction using cryptographically enforced boundaries. It ensures that models, data, workflows, reasoning steps, and operational logic cannot escape or violate the Privacy Domain constraints. It defines mechanisms for lawful computation, auditability, and control over AI operations, machine-learning inference, multi-agent plans, and transaction workflows. Operationalizes the most essential trust principles of the entire QPN ecosystem.

Applies to cloud providers, AI model operators, enclave-computing vendors, security platforms, compliance tools, and cross-border regulatory environments. It enables safe AI deployment, compliant data-processing, and cross-domain computation using verifiable privacy boundaries that surpass traditional enclave and federated-learning models.

Claim 15. A system comprising, in any operable combination, one or more of:

(a) a **QPC-governed execution engine** enforcing all computation inside a Privacy Domain;
(b) a **boundary-control module** verifying that computation conforms to Trust Criteria, jurisdictional mandates, or contractual restrictions;
(c) an **audit-generation engine** emitting Proof-of-Trust lineage for execution steps;
(d) a **cryptographic sealing layer** binding computation results to provenance metadata; and
(e) a **policy-routing module** determining permissible code paths;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 16. The system of Claim 15 wherein **QPC-governed execution restricts access to sensitive data, model parameters, or internal states.**

Claim 17. The system of Claim 15 wherein **lawful computation is enforced through a combination of Trust Criteria, policy weights, and governance constraints.**

Claim 18. The system of Claim 15 wherein **policy routing supports conditional execution based on participant jurisdiction or entitlement.**

Claim 19. The system of Claim 15 wherein **execution audit trails include lineage-based verification of safety or compliance events.**

Claim 20. The system of Claim 15 wherein **the execution engine prevents cross-domain leakage by encrypting intermediate computations.**

Claim 21. The system of Claim 15 wherein **boundary control prevents side-channel or inference attacks.**

Claim 22. The system of Claim 15 wherein **execution engines are certified using Proof-of-Trust to validate lawful behavior.**

Claim 23. The system of Claim 15 wherein **computation includes model inference, multi-agent reasoning, or transactional evaluation.**

Claim 24. **A method comprising**:

(a) executing computation under QPC-governed boundaries;
(b) enforcing Trust Criteria, policy constraints, or lawful-computation rules;
(c) generating audit lineage;
(d) cryptographically sealing results; and
(e) routing permissible outputs;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust

Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Family 1.3 — Inter-QPC Agreements, Delegation, Authority & Rights Propagation

This Family covers the creation, enforcement, and propagation of Inter-QPC Agreements that govern how rights, obligations, entitlements, authority, and capabilities pass between QPCs. These agreements ensure that multi-party workflows can execute securely without revealing private information. Rights may include access permissions, computation authority, contractual entitlements, financial rights, or operational delegation. All agreements are stored as Trust Blocks and enforced across the Privacy Graph.

Claim 25. A system comprising, in any operable combination, one or more of:

(a) an **Inter-QPC Agreement engine** defining rights, obligations, and delegation chains;

(b) a **propagation module** distributing agreement updates across dependent QPCs;

(c) a **compliance-verification engine** validating authority under Trust Criteria;

(d) a **cryptographic binding module** sealing agreements to Trust Blocks; and

(e) a **reallocation engine** modifying authority or entitlements based on updated lineage;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 26. The system of Claim 25 wherein **Inter-QPC Agreements govern access rights, contractual fulfillment, or computational authority.**

Claim 27. The system of Claim 25 wherein **authority propagation includes multi-hop delegation chains.**

Claim 28. The system of Claim 25 wherein **reallocation occurs automatically when upstream Trust Blocks indicate changing compliance or entitlement conditions.**

Claim 29. The system of Claim 25 wherein **agreements include privacy-preserving constraints preventing disclosure of counterparties.**

Claim 30. The system of Claim 25 wherein **authority expiration or renewal is determined through Proof-of-Trust lineage.**

Claim 31. A method comprising:

(a) defining an Inter-QPC Agreement;

(b) cryptographically binding rights or obligations to Trust Blocks;

(c) propagating agreement updates;

(d) verifying authority under Trust Criteria; and
(e) reallocating entitlements as required;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Family 1.4 — PPN/EPN Relationships & Domain Isolation

Covers how Personal Privacy Networks (PPNs) and Enterprise Privacy Networks (EPNs) interoperate with QPCs while maintaining strict isolation across domains. Each PPN and EPN relies on a private QPC-bound Privacy Domain that governs application access, data visibility, identity, rights management, and consent. Cross-domain interactions must occur through EasyAccess workflow threads or Inter-QPC Agreements, ensuring no domain can directly view or extract private data from another domain without lawful authorization. Applies to enterprise identity systems, consumer privacy frameworks, federated health systems, cloud multi-tenant architectures, and regulatory compliance platforms. The PPN/EPN domain model allows enterprises to adopt QPN capabilities without losing internal governance or autonomy.

Claim 32. A system comprising, in any operable combination, one or more of:

(a) a **Personal Privacy Network** anchored to a participant's QPC;
(b) an **Enterprise Privacy Network** anchored to an enterprise QPC;
(c) a **domain-isolation layer** preventing cross-domain data leakage;
(d) an **access-governance engine** resolving rights under Trust Criteria; and
(e) an **interaction-routing module** enforcing domain-specific policies;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 33. The system of Claim 32 wherein **PPNs govern individualized AI, messaging, identity, and rights management.**

Claim 34. The system of Claim 32 wherein **EPNs govern enterprise-level workflows, computational authority, and workforce management.**

Claim 35. The system of Claim 32 wherein **interactions between PPNs and EPNs occur only through Inter-QPC Agreements or EasyAccess workflows.**

Claim 36. The system of Claim 32 wherein **domain isolation prevents enterprise systems from retrieving personal identifiers, behavioral data, or private attributes.**

Claim 37. **A method comprising**:

(a) anchoring participant and enterprise workflows to respective QPCs;
(b) enforcing Privacy Domain boundaries;

(c) routing cross-domain interactions through Trust-Criteria-governed workflows;
(d) applying jurisdictional or contractual constraints; and
(e) generating verifiable lineage for each interaction;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

GROUP 2: TRUST BLOCKS, TRUST CRITERIA & PROOF-OF-TRUST (Claims 38-63)

This Group defines the cryptographically verifiable foundation of the Quantum Privacy Network (QPN). Trust Blocks, Trust Criteria, and Proof-of-Trust (PoT) comprise the enforceable policy and provenance substrate through which the network evaluates identity, rights, obligations, compliance, and lawful computation. They enable multi-party interaction, consent governance, jurisdiction enforcement, provenance integrity, and policy alignment across QPC-governed Privacy Domains without revealing private or proprietary information. They underpin every subsequent Group in the CIP.

Family 2.1 — Trust Blocks & Verifiable Provenance Records

This Family covers the mechanisms for creating, storing, sealing, and distributing Trust Blocks—cryptographically verifiable records that encode identity, provenance, consent, regulatory attributes, lineage, computation history, delegation, and compliance events. Trust Blocks ensure that all assertions or actions across the QPN are verifiable, immutable, privacy-preserving, and enforceable across multi-party workflows. They serve as the audit trail, lineage substrate, and authoritative truth source for identity, computation, policy, and multi-jurisdictional enforcement.

Claim 38. A system comprising, in any operable combination, one or more of:

(a) a **Trust Block generation engine** configured to create cryptographically verifiable records of identity, provenance, rights, obligations, or consent;
(b) a **sealing module** cryptographically binding Trust Blocks to QPC-enforced Privacy Domains;
(c) a **lineage-tracking engine** encoding time-ordered relationships among Trust Blocks;
(d) a **jurisdiction-encoding module** attaching regulatory or geographic attributes; and
(e) a **distribution layer** propagating Trust Blocks across compliant QPCs;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 39. The system of Claim 38 wherein **Trust Blocks encode consent lineage, provenance lineage, or computational lineage.**

Claim 40. The system of Claim 38 wherein **Trust Blocks include encrypted identifiers that preserve anonymity while allowing policy enforcement.**

Claim 41. The system of Claim 38 wherein **sealing prevents modification, deletion, or unauthorized disclosure of Trust Block contents.**

Claim 42. The system of Claim 38 wherein **Trust Blocks incorporate rights and obligations derived from Inter-QPC Agreements.**

Claim 43. The system of Claim 38 wherein **Trust Blocks include attestations for policy compliance or computational integrity.**

Claim 44. The system of Claim 38 wherein **Trust Blocks are chained using cryptographic lineage to prevent tampering or reordering.**

Claim 45. A method comprising:

(a) generating a Trust Block;
(b) binding it to a QPC-governed Privacy Domain;
(c) encoding lineage metadata;
(d) applying regulatory attributes; and
(e) distributing the Trust Block to authorized QPCs;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Family 2.2 — Trust Criteria: Rights, Consent, Jurisdiction & Obligations

Defines the structure and enforcement of Trust Criteria—machine-interpretable rules governing rights, obligations, consent, provenance, risk, and compliance. Trust Criteria govern what a QPC is allowed to do, and what Trust Credentials are necessary to authorize access to or use of QP Resources or their Resource Derivatives: what it can access, compute, delegate, modify, authorize, or disclose. They incorporate jurisdictional rules, regulatory requirements, contractual restrictions, fiduciary duties, environmental constraints, payment and licensing terms, policy mandates, authorized recipients, authorized purposes of use, semantic interoperability requirements, etc. Trust Criteria enable consistent cross-domain enforcement without exposing sensitive data.

Claim 46. A system comprising, in any operable combination, one or more of:

(a) a **Trust-Criteria definition engine** generating machine-interpretable rights, obligations, consent requirements, or policy constraints;
(b) a **jurisdiction-resolution module** determining applicable rules based on participant attributes;
(c) a **consent-governance engine** evaluating consent lineage and revocation;

(d) a **rights-enforcement module** restricting computation or access; and
(e) a **Trust-Criteria propagation engine** distributing updates across QPCs;

Wherein the system executes within QPC-enforced Privacy Domains comprising QPCs, Privacy Domains, Trust Criteria, Proof-of-Trust, Trust Blocks, or EasyAccess workflow threads.

Claim 47. The system of Claim 46 wherein **Trust Criteria encode regulatory, fiduciary, contractual, ethical, environmental, or safety constraints.**

Claim 48. The system of Claim 46 wherein **Trust Criteria determine permissible computation, routing, delegation, or disclosure.**

Claim 49. The system of Claim 46 wherein **consent lineage determines ongoing eligibility to access resources.**

Claim 50. The system of Claim 46 wherein **jurisdictional constraints enforce geographic-specific rights or obligations.**

Claim 51. The system of Claim 46 wherein **Trust Criteria updates trigger re-evaluation of QPC authority.**

Claim 52. **A method comprising:**
(a) defining Trust Criteria;
(b) applying jurisdictional rules;
(c) evaluating consent lineage;
(d) enforcing rights and obligations; and
(e) propagating Trust Criteria updates to dependent QPCs;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Family 2.3 — Proof-of-Trust (PoT) & Lineage Enforcement

This Family covers the mechanisms that generate, validate, and enforce Proof-of-Trust attestations, which certify that computation, access, delegation, consent, and policy-governed behavior occurred in compliance with Trust Criteria. PoT creates immutable, cryptographically verifiable evidence of lawful computation and policy enforcement, enabling multi-party trust without revealing underlying data.

Claim 53. A system comprising, in any operable combination, one or more of:

(a) a **Proof-of-Trust generation engine** producing verifiable attestations of rights enforcement, consent evaluation, computation, or policy compliance;
(b) a **lineage-verification module** confirming the integrity of Trust Block sequences;
(c) a **compliance-validation layer** comparing actions against Trust Criteria;
(d) a **cryptographic attestation layer** binding PoT outputs to computation; and

(e) a **PoT-distribution module** propagating attestations to authorized QPCs;

Wherein the system executes within QPC-enforced Privacy Domains comprising QPCs, Privacy Domains, Trust Criteria, Proof-of-Trust, Trust Blocks, or EasyAccess workflow threads.

Claim 54. The system of Claim 53 wherein **PoT records certify lawful computation or policy-aligned reasoning.**

Claim 55. The system of Claim 53 wherein **PoT includes selectively disclosed, privacy-preserving audit metadata.**

Claim 56. The system of Claim 53 wherein **lineage-verification ensures that Trust Blocks reflect unbroken, chronological provenance.**

Claim 57. The system of Claim 53 wherein **PoT includes attestations applicable to AI-agent behavior or autonomous automated systems.**

Claim 58. **A method comprising**:

(a) generating Proof-of-Trust attestations;
(b) verifying lineage;
(c) validating compliance with Trust Criteria;
(d) binding attestations to computation results; and
(e) distributing PoT outputs;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Family 2.4 — Multi-Domain Policy Enforcement & Compliance Control

This Family defines how QPCs enforce compliance rules across multiple domains—legal, contractual, fiduciary, ethical, environmental, and organizational. It ensures that policies encoded as Trust Criteria and AGPW weights are consistently applied to all cross-domain workflows, including transactions, agent interactions, AI inference, and distributed operations.

Claim 59. A system comprising, in any operable combination, one or more of:

(a) a **policy-enforcement engine** executing Trust Criteria across QPC-governed workflows;
(b) a **compliance-monitoring layer** detecting violations or anomalies;
(c) an **adaptive-routing module** directing workflows to compliant participants;
(d) a **multi-domain constraint evaluator** applying regulatory, contractual, or jurisdictional rules; and
(e) a **violation-recording engine** generating Trust Blocks documenting compliance events;

Wherein the system executes within QPC-enforced Privacy Domains comprising QPCs, Privacy Domains, Trust Criteria, Proof-of-Trust, Trust Blocks, or EasyAccess workflow threads.

Claim 60. The system of Claim 59 wherein **compliance monitoring triggers fallback or substitution workflows.**

Claim 61. The system of Claim 59 wherein **policy enforcement includes rule-based, conditional, or AGPW-weighted constraints.**

Claim 62. The system of Claim 59 wherein **violation records propagate as Trust Blocks across dependent QPCs.**

Claim 63. **A method comprising:**

(a) enforcing Trust Criteria;
(b) detecting compliance events;
(c) routing workflows to compliant participants;
(d) applying multi-domain constraints; and
(e) generating violation records as Trust Blocks;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

GROUP 3 — EASYACCESS INFRASTRUCTURE (Claims 64-85)

EasyAccess (EA) is the activation and routing layer that allows any participant, device, application, or enterprise system to interact with the Quantum Privacy Network without requiring integration, identity exchange, or exposure of personal or proprietary data. It provides the universal “entry point” for QPC-governed interaction by encapsulating identity, consent, and Trust Criteria evaluation inside a Privacy Domain rather than at the application perimeter. EasyAccess transforms ordinary links, messages, applications, or workflow triggers into privacy-preserving onboarding, authorization, and routing mechanisms that activate QPCs, propagate consent lineage, and establish trust-verified interactions across the network.

The core function of EA is to abstract away the customary integration burden that makes secure access slow, expensive, and fragmented across industries. In the QPX architecture, a simple EA trigger—embedded in a link, QR code, NFC token, or shareable object—initiates a QPC-governed process that automatically evaluates consent, jurisdiction, identity attributes, and rights, before routing the participant into a controlled workflow. This eliminates the need for enterprises to perform identity resolution, manage PII, or handle compliance-sensitive data directly.

EasyAccess also enables the viral propagation and distribution of governed workflows. Because EA links are encoded with privacy-preserving personalization metadata, they can

be shared through messaging, social platforms, collaboration tools, or enterprise systems while retaining strong guarantees of privacy, provenance, and compliance. Every propagation event generates Trust Blocks and Proof-of-Trust attestations, creating a complete lineage record across multi-hop sharing chains. Combined with QPC instantiation logic, EasyAccess becomes the central scaling primitive that allows QPX adoption to grow organically across participants, industries, and platforms while maintaining strong policy enforcement and cryptographic integrity.

From a systems perspective, EA represents a universal abstraction layer that harmonizes identity, trust, routing, and consent across thousands of applications and endpoints. It removes the need for enterprises to adopt new protocols, refactor systems, or create bilateral integrations. Within the QPX ecosystem, EasyAccess is the mechanism that translates the theoretical properties of privacy-preserving trust verification into a practical, zero-friction interaction model that works across all channels and contexts.

Family 3.1 — EasyAccess Links & Zero-Integration Activation

Addresses the mechanism by which a simple trigger—such as a URL, QR code, NFC gesture, or application-level share action—activates a QPC-governed workflow. The key innovation is that EasyAccess triggers operate without requiring any integration by the receiving application or service. Instead, the QPC interprets encrypted metadata inside the EA object, evaluates Trust Criteria, resolves jurisdiction, and establishes the user's rights or obligations without revealing identity or personal attributes to the destination system.

These claims establish that EA acts as the universal on-ramp to the QPX architecture. Whether the trigger is embedded in a clinical workflow, a supply-chain record, an online form, a device interface, or a consumer-facing website, the underlying system does not need to support QPN natively. The QPC does all the work, ensuring that the receiving application never touches sensitive identifiers, behavioral attributes, or regulatory metadata. This decoupling enables enterprises to adopt advanced privacy-preserving workflows instantly, without modifying existing systems.

Claim 64. A system comprising, in any operable combination:

(a) an **EasyAccess trigger** encoded within a URL, QR code, visual code, or machine-readable token;

(b) an **activation engine** configured to evaluate the trigger within a QPC-governed Privacy Domain;

(c) an **authorization layer** binding the activation to Trust Criteria lineage; and

(d) a **redirection module** routing to a resource or workflow without revealing identity or metadata;

Wherein execution occurs within QPN infrastructure comprising QPCs, Privacy Domains, Trust Criteria, Proof-of-Trust, Trust Blocks, or EasyAccess workflow threads.

Claim 65. The system of Claim 64 wherein the **EA trigger activates without server-side integration or application modification.**

Claim 66. The system of Claim 64 wherein **EA activation instantiates or activates a Personal Privacy Network.**

Claim 67. The system of Claim 64 wherein the **EA trigger includes encrypted personalization metadata interpretable only within a Privacy Domain.**

Claim 68. The system of Claim 64 wherein **EA activation generates a Trust Block documenting consent lineage.**

Claim 69. The system of Claim 64 wherein **EA triggers can be embedded into applications, messages, advertisements, or UI components.**

Claim 70. **A method comprising:**

(a) generating an EA trigger;
(b) evaluating the trigger within a Privacy Domain;
(c) binding activation to Trust Criteria; and
(d) routing the user to an authorized workflow;

Wherein activation reveals no personal identifiers to the destination.

Family 3.2 — Dual-Use Conversion of Apps, APIs & Platforms

Expands EasyAccess beyond simple triggers, enabling any existing application, website, SaaS platform, or API to function in "dual-use" mode—serving both as a conventional system and as a QPC-governed relying party without requiring code changes. This is achieved through protocol-mapping layers and QPC-mediated privacy boundaries that interpret application interactions as trusted, governed, and privacy-preserving workflows.

The system allows enterprises with large legacy estates—banks, insurers, healthcare providers, logistics networks, e-commerce platforms—to instantly transform their existing digital infrastructure into regulated, privacy-preserving onboarding and interaction surfaces. The underlying application remains unaware of the user's identity and never directly receives sensitive information. Instead, the QPC mediates all rights, obligations, consent lineage, and policy enforcement.

This converts the world's existing applications into trust-verifiable surfaces with no integration burden and no security risk to the enterprise. It shifts the paradigm from enterprise-centric control of data to participant-centric privacy domains governed by Trust Criteria, while giving enterprises a regulated, compliant, and future-proof interaction layer.

Claim 71. A system comprising, in any operable combination:

(a) a **dual-use conversion module** that enables an unmodified application, website, SaaS platform, or API to function as an EasyAccess Relying Party;

(b) a **protocol-mapping layer** converting app interactions into QPC-governed Trust-Criteria evaluations;
(c) a **privacy-preserving personalization engine** processing PPN attributes within a Privacy Domain; and
(d) a **compliance-verification engine** issuing Proof-of-Trust attestations for converted workflows;

Wherein execution occurs within QPC-governed Privacy Domains.

Claim 72. The system of Claim 71 wherein **dual-use conversion is enabled via configuration rather than code modification.**

Claim 73. The system of Claim 71 wherein **the platform's identity flows are replaced by EA activation.**

Claim 74. The system of Claim 71 wherein **the application remains unaware of user identity or PPN attributes.**

Claim 75. The system of Claim 71 wherein **EA conversion enables a platform to trigger QPC-governed consent or rights assertions.**

Claim 76. The system of Claim 71 wherein **the platform gains the ability to request Trust-Criteria-governed access without seeing underlying personal data.**

Claim 77. **A method comprising:**

(a) configuring an app or API as a dual-use EA endpoint;
(b) mapping authorization logic to Trust Criteria;
(c) invoking QPC workflows; and
(d) issuing privacy-preserving attestations;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Family 3.3 — EA Messaging, Social Propagation & Viral Routing

Governs the viral propagation capability of EasyAccess. Once generated, an EA trigger can be shared across messaging apps, social networks, email, collaboration platforms, or direct interpersonal interactions. Each share event is interpreted inside the recipient's QPC as a privacy-preserving, Trust-Criteria-governed workflow. Identity remains fully protected, yet lineage is preserved through Trust Blocks, enabling complete traceability and accountability across multi-hop propagation paths.

The claims in this family define how personalization occurs on a per-user basis within each QPC Privacy Domain. As EA content propagates, the QPC dynamically re-personalizes it based on consent, policy, preferences, and rights without modifying the surface content of the EA link. This enables governed workflows—healthcare actions, financial steps,

compliance tasks, engagement flows—to spread organically through human networks while preserving privacy, auditability, and lawful governance.

This allows QPX adoption to scale naturally through existing digital ecosystems. A participant can share a link in a text message, a clinician can share an authorization with a patient, a merchant can send a governed offer, or a government can distribute benefits—all without exposing personal data and without requiring platform-level support.

Claim 78. A system comprising, in any operable combination:

(a) a **propagation engine** enabling EA triggers to spread through messaging platforms, social networks, collaboration tools, or communication channels;
(b) a **context-personalization layer** deriving anonymous preferences from PPN policies;
(c) a **lineage-recording engine** generating Trust Blocks documenting propagation; and
(d) a **viral-routing module** allocating contribution value or incentives;

Wherein propagation occurs without revealing identity to platforms or intermediaries.

Claim 79. The system of Claim 78 wherein **EA triggers remain indistinguishable from ordinary URLs.**

Claim 80. The system of Claim 78 wherein **EA propagation supports multi-hop lineage across networks.**

Claim 81. The system of Claim 78 wherein **value allocation rewards Builders, Distributors, and Recipients participating in propagation.**

Claim 82. The system of Claim 78 wherein **EA content dynamically re-personalizes per recipient within Privacy Domains.**

Claim 83. The system of Claim 78 wherein **propagation includes QR, NFC, images, share-cards, or visual codes.**

Claim 84. The system of Claim 78 wherein **propagation events trigger QPC instantiation, activation, or Trust-Criteria evaluation.**

Claim 85. **A method comprising:**

(a) distributing EA content across digital channels;
(b) re-personalizing content within PPN-governed Privacy Domains;
(c) recording propagation lineage; and
(d) invoking Trust-Criteria-governed workflows;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

GROUP 4 — QPC LIFECYCLE AUTOMATION & PROPAGATION MECHANISMS (Claims 86-130)

Group 4 defines the lifecycle architecture that governs how Quantum Privacy Cells (QPCs) are created, activated, suspended, entangled, propagated, and retired across the Quantum Privacy Network. If Group 1 establishes the existence of Privacy Domains, and Group 2 defines how trust and policy are encoded within them, Group 4 is the operational scaffolding that ensures those constructs remain valid, synchronized, and enforceable across time, across participants, and across networks. These lifecycle mechanisms ensure that every action inside the QPN—identity use, consent, delegation, computation, or economic exchange—occurs within a QPC that is both cryptographically valid and policy-aligned.

The lifecycle system automates every state transition of a QPC. Upon instantiation, a QPC binds rights, obligations, jurisdiction, consent lineage, and Trust Criteria into a sealed Privacy Domain. Activation requires eligibility signals derived from Trust Blocks and Proof-of-Trust attestations, ensuring that only lawful, policy-compliant QPCs become operational, and that they are only used for lawful purposes. Suspension and retirement are triggered automatically by violations, revocations, expired consents, or governance updates. These transitions propagate to dependent QPCs, guaranteeing that any authorization chain or delegated authority remains synchronized across the network.

A second foundational aspect of Group 4 is QPC interdependency and entanglement. QPCs rarely operate in isolation. They form chains of delegation, shared authority, multi-party workflows, and joint resource usage. Group 4 formalizes how lineage, entanglement, and dependency structures are encoded and maintained. When the state of one QPC changes—activated, suspended, revoked—those transitions propagate across entangled QPCs, ensuring that no orphaned or inconsistent trust states persist across the network. This maintains the integrity of distributed workflows without exposing identity or sensitive data.

Finally, Group 4 establishes the population-scale governance layer for lifecycle management. The QPX ecosystem may contain millions or even billions of QPCs operating concurrently. This Family ensures that global governance signals—policy changes, AGPW updates, jurisdictional shifts, risk detection, revocations—can be applied across entire populations in a privacy-preserving, lineage-verifiable manner. It provides the architectural backbone that keeps the network coherent at scale, aligning QPC authority and capability ceilings with human-managed governance and automated Trust Criteria evaluation.

Group 4 transforms the QPN from a static trust substrate into a living, adaptive, self-governing privacy ecosystem capable of secure global-scale operation.

Family 4.1 – Automated QPC Creation, Activation, Suspension & Retirement

Governs the full lifecycle of a QPC: how it comes into existence, how it is activated, and how its operational authority changes over time. When a QPC is instantiated, it binds identity attributes, consent lineage, rights, obligations, and jurisdictional metadata into a cryptographically sealed Privacy Domain. Activation requires the QPC to satisfy Trust Criteria, ensuring that only lawful, policy-aligned QPCs gain access to computation, resources, or workflows. Suspension and retirement are triggered automatically by violations, expirations, or revocations—providing an elegant enforcement mechanism that scales without human intervention.

The lifecycle controller ensures that every QPC transition is captured through Trust Blocks and Proof-of-Trust attestations. These attestations become the authoritative record of eligibility and compliance. When a QPC is suspended or retired, all associated rights, obligations, and delegated authorities are revoked or transitioned. Downstream workflows, resource allocations, or multi-party interactions automatically adjust, ensuring that no stale or unauthorized authority remains active in the system.

Claim 86. A system comprising, in any operable combination:

(a) a **QPC-instantiation engine** configured to create a Quantum Privacy Cell for a participant, device, enterprise, agent, or workflow;
(b) a **rights-binding module** attaching Trust Criteria, jurisdiction, consent lineage, and policy constraints to the newly instantiated QPC;
(c) an **activation engine** that transitions the QPC into an operational state based on eligibility signals; and
(d) a **lifecycle controller** managing QPC suspension, reactivation, or retirement;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 87. The system of Claim 86 wherein **QPC instantiation is triggered by EasyAccess activation, onboarding, identity verification, or workflow initiation.**

Claim 88. The system of Claim 86 wherein **QPC activation requires satisfaction of Trust Criteria including jurisdictional, contractual, or regulatory thresholds.**

Claim 89. The system of Claim 86 wherein **QPC suspension is triggered by violation of consent lineage, Trust Criteria, PoT signals, or detected non-compliance.**

Claim 90. The system of Claim 86 wherein **QPC retirement seals the Privacy Domain, finalizes lineage, terminates entitlements, and archives Trust Blocks.**

Claim 91. The system of Claim 86 wherein **lifecycle transitions generate Proof-of-Trust attestations and updated Trust Blocks documenting state changes.**

Claim 92. The system of Claim 86 wherein **retirement prevents any future activation of computation, disclosure, delegation, or authority.**

Claim 93. The system of Claim 86 wherein **suspension or retirement revokes rights and obligations encoded in Inter-QPC Agreements.**

Claim 94. The system of Claim 86 wherein **QPC lifecycle triggers automated notifications to dependent QPCs, workflows, or Exchange Networks.**

Claim 95. The system of Claim 86 wherein **lifecycle transitions propagate across entangled or dependent QPCs based on lineage relationships.**

Claim 96. **A method comprising:**

(a) instantiating a QPC;
(b) binding rights, obligations, jurisdiction, and consent lineage;
(c) activating the QPC upon satisfying Trust Criteria;
(d) suspending or retiring the QPC upon violation or expiration of eligibility; and
(e) generating Proof-of-Trust attestations for each transition;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 97. The method of Claim 96 wherein **QPC instantiation automatically generates an initial lineage Trust Block.**

Claim 98. The method of Claim 96 wherein **QPC activation triggers provisioning of cryptographically bounded computational authority.**

Claim 99. The method of Claim 96 wherein **QPC retirement prevents any further execution, claiming, delegation, or access to resources.**

Claim 100. The method of Claim 96 wherein **lifecycle transitions are propagated to dependent QPCs for compliance alignment or authority recalibration.**

Family 4.2 — QPC Interdependency, Entanglement & Propagation

The entanglement architecture manages how QPCs form dependency chains. In the QPX ecosystem, workflows frequently require multiple participants, each operating their own QPC. These QPCs may depend on shared resources, delegated authority, contractual relationships, or shared lineage metadata. This Family ensures that these dependency structures are recorded as Trust Blocks and that any state change in one QPC—activation, revocation, suspension—propagates lawfully and consistently across all entangled QPCs.

Entanglement establishes a lineage-driven trust structure across multi-hop interactions. If a delegated authority becomes invalid, if consent lineage changes, or if contractual

constraints update, these signals propagate in real time to all dependent QPCs. This prevents stale credentials, unauthorized access, or policy violations from persisting undetected. It also enables distributed workflows to operate safely, because every dependent QPC continually recalibrates its permissible actions based on upstream Trust Criteria changes.

Claim 101. A system comprising, in any operable combination:

(a) an **entanglement-mapping engine** configured to record interdependencies among Quantum Privacy Cells (QPCs) using Trust Blocks;
(b) a **propagation engine** that distributes state changes, rights, obligations, or eligibility updates across entangled QPCs;
(c) a **lineage-analysis module** determining multi-hop dependency paths; and
(d) a **policy-alignment module** enforcing Trust Criteria consistently across dependent QPCs;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 102. The system of Claim 101 wherein **entanglement is established when QPCs share rights, obligations, computational authority, contractual lineage, or delegated responsibilities.**

Claim 103. The system of Claim 101 wherein **propagation includes changes to eligibility, jurisdictional authority, consent lineage, or compliance state.**

Claim 104. The system of Claim 101 wherein **multi-hop propagation occurs through lineage-based dependency structures encoded in Trust Blocks.**

Claim 105. The system of Claim 101 wherein **entanglement relationships are dynamically updated as delegation chains, agreements, or resource allocations evolve.**

Claim 106. The system of Claim 101 wherein **propagation includes revocation of authority or rights when an upstream QPC violates Trust Criteria.**

Claim 107. The system of Claim 101 wherein **propagation triggers recalibration of Trust Criteria across dependent QPCs.**

Claim 108. The system of Claim 101 wherein **entanglement supports distributed workflows in which multiple QPCs collectively execute a governed operation.**

Claim 109. The system of Claim 101 wherein **entanglement lineage determines permissible routing for computation, delegation, or authority transfer.**

Claim 110. The system of Claim 101 wherein **propagation includes suspension or contraction of downstream capabilities when the upstream source is suspended.**

Claim 111. The system of Claim 101 wherein **updates to consent lineage propagate to all dependent QPCs to ensure continued lawful computation.**

Claim 112. The system of Claim 101 wherein **entanglement metadata is represented as privacy-preserving, selectively disclosed attributes.**

Claim 113. **A method comprising:**

(a) establishing entanglement among QPCs based on rights, obligations, or lineage metadata;
(b) encoding entanglement relationships in Trust Blocks;
(c) propagating state changes across dependent QPCs;
(d) enforcing Trust Criteria during propagation; and
(e) generating Proof-of-Trust attestations documenting propagation events;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 114. The method of Claim 113 wherein **propagation includes updating multi-hop dependency chains.**

Claim 115. The method of Claim 113 wherein **changes to jurisdiction, consent, or eligibility propagate automatically to maintain cross-domain compliance.**

Family 4.3 — Population-Scale QPC Governance, Monitoring & Dynamic Reallocation

Defines the global oversight model for millions or billions of QPCs operating concurrently. It establishes a population-level governance engine that monitors QPC eligibility, compliance, lifecycle state, and risk signals derived from lineage-based analytics. When a QPC becomes non-compliant or ineligible, or when global governance rules change, the system recalibrates authority and eligibility automatically. In distributed workflows, responsibilities can be reallocated to compliant QPCs without pausing or disrupting operations.

This Family also governs dynamic governance propagation: jurisdictional shifts, updated Trust Criteria, AGPW weighting changes, or revocation events are distributed across the dependent QPC network through lineage-based propagation. This ensures the entire QPX ecosystem remains synchronized with current legal, regulatory, ethical, and operational requirements. It is the architectural foundation that allows the network to remain safe, lawful, and resilient even under rapid policy change or adversarial conditions.

Claim 116. A system comprising, in any operable combination:

(a) a **population-governance engine** configured to monitor lifecycle, eligibility, compliance, and Trust-Criteria states across multiple QPCs;
(b) a **risk-detection module** identifying anomalies, violations, or failure signals based on Proof-of-Trust lineage;
(c) an **eligibility-recalibration module** evaluating whether QPCs remain authorized to act under jurisdictional or contractual constraints;
(d) a **reallocation engine** assigning responsibilities, delegation chains, entitlements, or workflow roles to alternative QPCs; and
(e) a **propagation module** distributing governance updates across dependent QPCs;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 117. The system of Claim 116 wherein **population-level monitoring includes aggregated, privacy-preserving analytics that exclude personal identifiers.**

Claim 118. The system of Claim 116 wherein **risk detection triggers suspension, revocation, or escalation workflows.**

Claim 119. The system of Claim 116 wherein **eligibility recalibration includes jurisdiction shifts, contractual updates, or consent lineage changes.**

Claim 120. The system of Claim 116 wherein **reallocation occurs when a QPC becomes non-compliant, suspended, revoked, or retired.**

Claim 121. The system of Claim 116 wherein **reallocation includes automatic substitution of authorized QPCs for affected roles.**

Claim 122. The system of Claim 116 wherein **multi-hop dependencies propagate governance outcomes across Lineage Graphs of QPCs.**

Claim 123. The system of Claim 116 wherein **population-governance updates generate new Trust Blocks documenting changes to lifecycle or authority.**

Claim 124. The system of Claim 116 wherein **QPC governance includes detection of systemic anomalies across a plurality of participants.**

Claim 125. The system of Claim 116 wherein **governance signals integrate with AGPW policy-weighting to modify permissible computation or routing.**

Claim 126. The system of Claim 116 wherein **governance includes maintaining capability ceilings for QPCs based on trust, safety, or compliance states.**

Claim 127. **A method comprising:**

(a) monitoring lifecycle and compliance conditions across QPC populations;
(b) detecting anomalies or violations using lineage-based analytics;

(c) recalibrating eligibility or authority under Trust Criteria;
(d) reallocating responsibilities to compliant QPCs; and
(e) propagating updated governance states across dependent QPCs;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 128. The method of Claim 127 wherein **recalibration includes suspension or retirement of non-compliant QPCs.**

Claim 129. The method of Claim 127 wherein **reallocation includes assigning jurisdiction-aware authority to alternative QPCs.**

Claim 130. The method of Claim 127 wherein **governance propagation is recorded as Proof-of-Trust lineage updates.**

GROUP 5 — QUANTUM RATING SYSTEM (QRS) (Claims 131–165)

The Quantum Rating System (QRS) provides the unified trust-scoring, lineage evaluation, and cross-domain normalization engine for the entire Quantum Privacy Network. While QPCs establish cryptographically sealed execution boundaries, and Trust Blocks preserve verifiable lineage, QRS is the mechanism that converts these primitives into actionable, dynamic trust metrics that guide access, routing, capability ceilings, incentives, and participation across the QPX ecosystem. QRS is the global "governance intelligence layer" that continuously recalibrates trust, safety, compliance, and contribution signals without exposing identity or regulated data.

QRS operates by drawing from the privacy-preserving metadata within each QPC—consent lineage, contractual constraints, jurisdictional requirements, provenance records, behavioral telemetry, and Proof-of-Trust attestations. It synthesizes these inputs into multi-dimensional trust metrics that determine what a participant, enterprise, resource, or AI agent is allowed to do at any moment. These trust ratings are recalculated continuously as behavior evolves, obligations change, risks emerge, or policy updates propagate through the network. This ensures that trust is not static but adaptively aligned with real-world conditions.

A key innovation of QRS is that it operates entirely within Privacy Domains, without revealing the underlying data that contributes to a rating. This enables cross-domain interactions—clinical, financial, consumer, enterprise, public-benefit—without collapsing privacy boundaries. The system normalizes ratings across domains and jurisdictions while still preserving context and regulatory requirements. QRS allows the network to reason about the eligibility, safety, and reliability of participants and assets at a global scale while maintaining absolute privacy fidelity.

Finally, QRS is the central enforcement mechanism for AGPW's policy weighting and for PPOS's optimization frameworks. Trust ratings are not simply informational; they directly govern the activation of workflows, the granting of resource access, the promotion or limitation of AI capabilities, and the routing of incentives. QRS therefore transforms the QPX from a passive trust infrastructure into a dynamic, self-governing system with measurable, verifiable, and adaptive trust signals.

Family 5.1 — Core Quantum Rating Engine

Family 5.1 defines the foundational rating engine that synthesizes multi-dimensional trust inputs into actionable Quantum Ratings. These inputs include identity proofs, contractual obligations, jurisdictional metadata, behavioral telemetry, provenance lineage, safety signals, and Proof-of-Trust attestations. The rating engine generates trust metrics that govern whether a participant, resource, or AI agent may perform a given action or access a given workflow. These metrics are continuously recalibrated as underlying conditions change, ensuring adaptive trust enforcement.

The claims in this Family also establish the privacy-preserving nature of QRS computation. All rating logic executes inside QPC Privacy Domains, ensuring that neither enterprises nor counterparties gain visibility into the inputs or internal mechanics of the rating computation. This preserves confidentiality while providing strong, auditable trust guarantees for every interaction.

Claim 131. A system comprising, in any operable combination:

(a) a **Quantum Rating engine** configured to compute multi-dimensional, privacy-preserving rating outputs for participants, resources, workflows, or agents;
(b) an **ingestion module** receiving encrypted provenance, consent, jurisdiction, and behavioral attributes from Trust Blocks;
(c) a **constraint-evaluation module** ensuring all rating computations comply with Trust Criteria; and
(d) a **sealing module** binding rating outputs to lineage metadata;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 132. The system of Claim 131 wherein **rating computations include trustworthiness, safety alignment, compliance, contribution value, and contextual eligibility.**

Claim 133. The system of Claim 131 wherein **the rating engine supports encrypted or zero-knowledge computation without revealing underlying feature values.**

Claim 134. The system of Claim 131 wherein **rating outputs are represented as multi-dimensional vectors tied to lineage provenance.**

Claim 135. The system of Claim 131 wherein **the engine evaluates jurisdictional constraints derived from Trust Criteria.**

Claim 136. The system of Claim 131 wherein **rating outputs adjust dynamically based on updated PoT attestations.**

Claim 137. The system of Claim 131 wherein **QPC-governed inputs include identity attributes, resource provenance, contractual rights, or environmental-impact metrics.**

Claim 138. The system of Claim 131 wherein **outputs are sealed into Trust Blocks for downstream routing or exchange.**

Claim 139. The system of Claim 131 wherein **rating computations include cross-domain signals aggregated without disclosing participant identity.**

Claim 140. **A method comprising:**

(a) ingesting encrypted or privacy-preserving inputs;
(b) evaluating Trust Criteria;
(c) computing multi-dimensional Quantum Rating values; and
(d) sealing rating outputs to lineage metadata;

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells; (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 141. The method of Claim 140 wherein **rating values are used to determine eligibility for workflows or access permissions.**

Claim 142. The method of Claim 140 wherein **rating computations incorporate historical lineage, consent changes, or jurisdiction shifts.**

Claim 143. The method of Claim 140 wherein **rating values update in real time based on incoming PoT attestations.**

Claim 144. The method of Claim 140 wherein **rating outputs propagate to dependent QPCs or Exchange Networks.**

Claim 145. The method of Claim 140 wherein **sealed rating outputs influence routing, prioritization, or AI capability ceilings.**

Family 5.2 — Lineage-Aware Multi-Dimensional Rating Models

Family 5.2 extends the rating engine by incorporating multi-lineage, multi-dimensional trust analysis. Instead of computing trust solely from the current state of a QPC, this Family establishes rating models that incorporate upstream lineage, historical obligations, behavioral evolution, social-benefit signals, and cross-domain provenance. These models evaluate trust at a deeper structural level, analyzing how multiple QPCs, interactions, or obligations interrelate across time and jurisdiction.

This approach enables the system to detect systemic risk, compliance erosion, or beneficial contribution patterns that would not be visible through single-QPC analysis. It allows QRS to treat trust as an evolving, contextual attribute—one that adapts to real-world conditions and cross-domain dependencies.

Claim 146. A system comprising, in any operable combination, one or more of:

(a) extracting multi-dimensional attributes from Trust Blocks;
(b) applying lineage-weighted scoring;
(c) aggregating dimension-specific metrics; and
(d) producing composite ratings inherited across derivative outputs.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 147. The system of Claim 146 wherein: **(a)** resource lineage graphs are traversed to compute cumulative trust; **(b)** constraints are propagated across upstream sources; and **(c)** weights reflect historical compliance evidence.

Claim 148. The system of Claim 146 wherein: **(a)** rating factors include provenance quality; **(b)** constraint strictness; **(c)** semantic accuracy; and **(d)** multi-party policy inheritance depth.

Claim 149. The system of Claim 146 wherein: **(a)** lineage-aware scoring adjusts weights for missing provenance; **(b)** detects unverifiable segments; and **(c)** reduces trust contributions from ambiguous sources.

Claim 150. The system of Claim 146 comprising: **(a)** multi-dimensional scoring across trust, compliance, safety, value, contribution, and risk dimensions; and **(b)** normalization across heterogeneous taxonomies via UTM mappings.

Claim 151. The system of Claim 146 wherein rating models: **(a)** ingest encrypted metrics; **(b)** compute scores without revealing underlying data; and **(c)** bind outputs to Trust Blocks with inherited constraints.

Claim 152. The system of Claim 146 wherein multidimensional scores: **(a)** are updated dynamically as lineage changes; **(b)** decay over time; and **(c)** reflect new provenance or compliance events.

Claim 153. The system of Claim 146 wherein: **(a)** multi-layer lineage structures are flattened into canonical rating paths; **(b)** circular dependencies are removed; and **(c)** inherited metrics are consolidated.

Claim 154. The system of Claim 146 wherein lineage-aware models: **(a)** treat upstream violations as negative modifiers; **(b)** propagate suspension flags; and **(c)** restrict downstream eligibility based on inherited Trust Criteria.

Claim 155. The system of Claim 146 wherein: **(a)** multi-dimensional vectors include contribution scoring for network effects; **(b)** account for secondary and tertiary lineage impacts; and **(c)** generate aggregated influence-weighted trust metrics.

Claim 156. The system of Claim 146 wherein lineage-aware models: **(a)** compute separate public-benefit dimensions; **(b)** track derivative-value propagation; and **(c)** embed PBDR-related weights into rating outputs.

Claim 157. The system of Claim 146 wherein: **(a)** policy-compliance dimensions are derived from mapped UTM taxonomies; **(b)** multi-party obligations are scored; and **(c)** cross-jurisdiction lineage segments receive differentiated weights.

Claim 158. The system of Claim 146 wherein: **(a)** weighting factors reflect contribution categories; **(b)** semantic descriptors; and **(c)** resource-utilization histories aggregated across lineage branches.

Claim 159. The system of Claim 146 wherein lineage-aware rating vectors: **(a)** inform routing decisions; **(b)** govern eligibility for Resource Pools and Exchange Networks; and **(c)** influence tokenized value allocation.

Family 5.3 — Cross-Domain Rating Normalization, Routing & Policy Alignment

Family 5.3 defines the mechanisms by which Quantum Ratings are normalized, interpreted, and applied across different sectors, jurisdictions, and workflow contexts. Because trust signals originate from diverse environments—clinical, financial, consumer, enterprise, government—they must be translated into a unified rating framework that can govern cross-domain workflows. This Family ensures that trust metrics travel with participants and resources as they move between sectors, without revealing sensitive data or violating regulatory boundaries.

The claims also establish how QRS integrates with AGPW and PPOS. Normalized ratings determine the capability ceilings for AI agents, the routing of optimization workflows, the eligibility of participants for particular actions, and the evaluation of systemic risk. The Family ensures that trust signals propagate consistently across the QPX architecture, serving as the common currency of governance, safety, and verification.

Claim 160. A system comprising, in any operable combination, one or more of:

(a) mapping heterogeneous rating dimensions to canonical UTM taxonomies;
(b) aligning scores from multiple domains; and
(c) producing unified routing metrics usable across Exchange Networks.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells; (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 161. The system of Claim 160 wherein: **(a)** cross-domain policies are compiled into normalized rating constraints; **(b)** conflicting obligations are resolved; and **(c)** equivalent criteria across jurisdictions are harmonized.

Claim 162. The system of Claim 160 wherein normalized scores: **(a)** support routing across Exchange Networks; **(b)** determine eligibility thresholds; and **(c)** drive automated policy alignment in cross-domain computation.

Claim 163. The system of Claim 160 wherein: **(a)** domain-specific deviations are corrected; **(b)** rating vectors are rescaled for cross-network comparability; and **(c)** multi-party lineage weights are normalized.

Claim 164. The system of Claim 160 wherein cross-domain normalized ratings: **(a)** govern multi-party routing; **(b)** constrain cross-jurisdiction execution; and **(c)** enforce alignment between provenance requirements and policy bundles.

Claim 165. The system of Claim 160 wherein normalized vectors: **(a)** enable stable cross-domain rating equivalence; **(b)** support adaptive rescaling under updated Trust Taxonomies; and **(c)** allow synchronized routing decisions across Exchange Networks.

GROUP 6 — ADAPTIVE GLOBAL POLICY WEIGHTING (AGPW) (Claims 166-210)

Adaptive Global Policy Weighting (AGPW) is the dynamic governance layer that ensures the Quantum Privacy Network continually aligns its behavior with evolving human values, legal standards, cross-jurisdictional policy frameworks, and environmental or societal outcomes. While QPCs enforce local constraints and Trust Blocks maintain immutable lineage, AGPW determines how governance signals—ethical parameters, regulatory mandates, safety constraints, economic priorities—are weighted, harmonized, and applied across the network in real time.

AGPW converts governance into an adaptive optimization problem. It continuously recalibrates how Trust Criteria, jurisdictional rules, QRS trust metrics, and Proof-of-Trust signals shape the behavior of participants, resources, AI agents, and workflows. Policy changes do not require hard-coded updates or enterprise integrations; they propagate automatically through QPC Privacy Domains, adjusting capability ceilings, eligibility rules, interaction pathways, and risk thresholds. This allows the network to remain aligned with legal, ethical, and societal expectations even as conditions change.

A unique strength of AGPW is its blend of decentralization and human oversight. Multiple Human-Managed Trust Authorities (HTAs)—representing ethical traditions, regulatory bodies, cultural contexts, industry frameworks, or environmental priorities—contribute weighted policy components. AGPW reconciles these diverse governance inputs into a coherent global weighting structure without imposing the values of any single entity. This "constitutional pluralism" allows the network to operate fairly across jurisdictions, cultures, and economic systems.

Finally, AGPW closes the governance loop through continuous feedback. Behavior across the network—AI outputs, participant actions, workflow outcomes, ecological or social

impacts—feeds back into QRS and PoT telemetry. AGPW uses this telemetry to adjust governance parameters dynamically. This creates a self-optimizing ecosystem where policy, behavior, trust, and incentives continually realign toward measurable public-good outcomes while preserving individual rights and privacy.

Family 6.1 — AGPW Policy-Inference Engine

Family 6.1 introduces the core inference engine that translates diverse governance inputs into actionable policy weightings. These governance inputs include legal rules, regulatory mandates, cultural norms, ethical values, environmental constraints, sector-specific frameworks, and dynamically measured outcomes. The inference engine harmonizes these inputs within QPC Privacy Domains, ensuring that local policy enforcement is consistent with global governance expectations.

The system does not merely read policy; it computes policy alignment as a dynamic function of Trust Criteria, QRS ratings, PoT lineage analytics, and behavioral telemetry. As new risks arise, as jurisdictions update rules, or as HTAs adjust governance parameters, the AGPW engine recalibrates the policy weights that govern interaction. This real-time recalibration ensures that the QPX ecosystem behaves as a continuously aligned, self-governing system.

Claim 166. A system comprising, in any operable combination, one or more of:

(a) **ingesting policy signals from Trust Blocks**;
(b) **deriving global policy-weight vectors**;
(c) **applying multi-factor inference models**; and
(d) **generating adaptive policy-weight outputs** usable across QPX governance layers.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells; (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 167. The system of Claim 166 wherein: **(a)** Trust Criteria define evaluative constraints; **(b)** inference models incorporate compliance, risk, safety, and contribution metrics; and **(c)** policy weights update as Trust Block evidence changes.

Claim 168. The system of Claim 166 wherein: **(a)** input signals include jurisdictional policies; **(b)** contractual constraints; and **(c)** ethical or fiduciary requirements mapped through UTM taxonomies.

Claim 169. The system of Claim 166 wherein: **(a)** policy inference incorporates lineage-aware evidence; **(b)** multi-party obligations; and **(c)** cross-source semantic descriptors affecting weight assignment.

Claim 170. The system of Claim 166 wherein: **(a)** inference rules incorporate historical compliance; **(b)** decay functions adjust outdated policy signals; and **(c)** absent evidence reduces weight confidence.

Claim 171. The system of Claim 166 wherein: **(a)** Trust Blocks define measurable indicators; **(b)** policy weights are computed through scalar or vector compositions; and **(c)** outputs are bound to downstream governance workflows.

Claim 172. The system of Claim 166 wherein: **(a)** policy inference integrates multi-domain evidence; **(b)** resolves conflicting policy signals; and **(c)** assigns weighted priorities aligned with UTM policy categories.

Claim 173. The system of Claim 166 wherein: **(a)** inference logic incorporates machine-evaluated Trust Criteria; **(b)** detects anomalous or contradictory policy evidence; and **(c)** adjusts weighting factors accordingly.

Claim 174. The system of Claim 166 wherein: **(a)** policy-weight outputs trigger routing decisions; **(b)** constrain allowable actions in runtime systems; and **(c)** govern eligibility for Resource Pools or Exchange Networks.

Claim 175. The system of Claim 166 wherein: **(a)** inferred weights incorporate public-benefit dimensions; **(b)** PBDR-related policy adjustments; and **(c)** constraints derived from redistributive governance logic.

Claim 176. The system of Claim 166 wherein: **(a)** Trust Criteria are used to parameterize inference models; **(b)** semantic descriptors serve as dimension selectors; and **(c)** weighted outputs influence downstream AGPW calculations.

Claim 177. The system of Claim 166 wherein: **(a)** UTM taxonomies define canonical policy domains; **(b)** lineage-derived attributes modify weight magnitudes; and **(c)** multi-authority constraints are encoded into inference pathways.

Claim 178. The system of Claim 166 wherein: **(a)** inference models integrate safety and risk metrics; **(b)** adjust for environmental, fiduciary, or societal priorities; and **(c)** reflect cross-sectoral policy demands.

Claim 179. The system of Claim 166 wherein: **(a)** policy inference identifies dominant influences; **(b)** maps oppositional criteria; and **(c)** produces stable weights through equilibrium-seeking logic.

Claim 180. The system of Claim 166 wherein: **(a)** multi-dimensional weight vectors are cryptographically bound; **(b)** tied to provenance; and **(c)** updated through continuous PoT verification.

Claim 181. The system of Claim 166 wherein: **(a)** policy-weight deltas are computed on new Trust Block arrivals; **(b)** lineage-aware changes propagate; and **(c)** downstream rating and governance layers receive updates in real time.

Claim 182. The system of Claim 166 wherein: **(a)** inference logic integrates conflict-resolution models; **(b)** suppresses contradictory signals; and **(c)** produces harmonized weight outputs.

Claim 183. The system of Claim 166 wherein: **(a)** inputs include normative, statutory, contractual, and ethical governance signals; **(b)** multi-authority semantics are aligned; and **(c)** weight vectors incorporate aggregated global policy influence.

Family 6.2 — Multi-Authority Governance, Pluralism & Harmonization

Formalizes a governance architecture in which multiple Human-Managed Trust Authorities contribute distinct policy frameworks that are harmonized through AGPW. This prevents any single political, corporate, or ideological entity from imposing unilateral control. Instead, governance emerges through weighted federation, where diverse legal, ethical, and cultural traditions are incorporated into the QPX ecosystem. Each HTA contributes policy components, and AGPW computes harmonized governance weights, ensuring both diversity and global alignment.

Ensures that governance operates with constitutional pluralism: baseline principles—privacy, human rights, safety, fairness—serve as global constraints, while more localized rules can be weighted differently across jurisdictions. This preserves legitimacy across global markets and regulatory environments while preventing inconsistent or conflicting governance from destabilizing the network.

Claim 184. A system comprising, in any operable combination, one or more of:

(a) aggregating governance inputs from multiple authorities;
(b) mapping diverse policy traditions to UTM taxonomies;
(c) generating harmonized governance-weight outputs; and
(d) producing multi-authority consensus indicators.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells; (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 185. The system of Claim 184 wherein: **(a)** cross-authority constraints are deconflicted; **(b)** overlapping requirements are merged; and **(c)** authority-specific divergences are captured as weighted differences.

Claim 186. The system of Claim 184 wherein: **(a)** pluralistic governance traditions are modeled as policy-weight distributions; **(b)** conflicting norms are resolved through UTM equivalence mappings; and **(c)** harmonized outputs preserve cross-jurisdictional legitimacy.

Claim 187. The system of Claim 184 wherein: **(a)** global, national, sectoral, and institutional authorities contribute independent governance signals; **(b)** these signals are normalized; and **(c)** combined into unified governance vectors.

Claim 188. The system of Claim 184 wherein: **(a)** minority-governance positions are preserved; **(b)** weighted influence is calculated; and **(c)** pluralistic representation is encoded into the harmonization logic.

Claim 189. The system of Claim 184 wherein: **(a)** multi-authority ratings identify compatible policy segments; **(b)** detect irreconcilable conflicts; and **(c)** perform selective constraint substitution.

Claim 190. The system of Claim 184 wherein: **(a)** governance-weight outputs reflect competing authority priorities; **(b)** derive shared governance equilibria; and **(c)** produce domain-specific consensus paths.

Claim 191. The system of Claim 184 wherein: **(a)** cross-authority trust signals are synthesized; **(b)** semantic descriptors align policy concepts; and **(c)** UTM mappings determine governance-weight compatibility.

Claim 192. The system of Claim 184 wherein: **(a)** successor authorities inherit governance weights; **(b)** lineage propagation updates harmonized constraints; and **(c)** authority transitions trigger recalculation.

Claim 193. The system of Claim 184 wherein: **(a)** contextual policy demands shape weighting factors; **(b)** policy bundles are compared across authorities; and **(c)** divergence signatures influence governance scores.

Claim 194. The system of Claim 184 wherein: **(a)** governance vectors include global and local authority components; **(b)** relative influence is computed; and **(c)** mapped to canonical UTM governance dimensions.

Claim 195. The system of Claim 184 wherein: **(a)** harmonization logic incorporates trust-weighted scoring; **(b)** accounts for authority legitimacy; and **(c)** circuit-breaks conflicting governance signals.

Claim 196. The system of Claim 184 wherein: **(a)** governance outputs feed AGPW policy weighting; **(b)** constrain runtime decisions; and **(c)** inform global equilibrium calculations.

Claim 197. The system of Claim 184 wherein: **(a)** cross-authority governance harmonization creates stable consensus envelopes; **(b)** encodes conflicting values into weighted distributions; and **(c)** ensures pluralistic governance representation.

Family 6.3 — Runtime Policy Execution, Feedback Loops & Equilibrium Enforcement

Establishes the runtime execution layer that operationalizes AGPW weightings. It ensures that as governance priorities shift, the network immediately adjusts participant capabilities, workflow routing, resource eligibility, and AI-agent authority. These adjustments are not static; they evolve continuously as the system monitors real-world behavior, evaluates PoT signals, updates QRS ratings, and measures cross-domain outcomes.

Implements the feedback architecture that keeps the network in governance equilibrium. When the network detects undesirable patterns—policy violations, systemic risks, harmful outputs, ecological degradation, inequitable outcomes—it recalibrates governance weights and adjusts capability ceilings. Conversely, beneficial behavior triggers positive adjustments. This guarantees that governance is not merely declarative but actively shaping the behavior of the ecosystem.

Claim 198. A system comprising, in any operable combination, one or more of:

(a) executing policy-weight vectors in runtime computation;
(b) enforcing AGPW-derived constraints;
(c) applying continuous feedback loops; and
(d) driving convergence toward global governance equilibrium.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells; (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 199. The system of Claim 198 wherein: **(a)** runtime decisions are adjusted using updated policy weights; **(b)** recalibration occurs on each Trust Block event; and **(c)** route selections follow AGPW-governed thresholds.

Claim 200. The system of Claim 198 wherein: **(a)** feedback signals include compliance, risk, and lineage events; **(b)** error-correction logic adjusts policy weights; and **(c)** equilibrium states are maintained through recursive updates.

Claim 201. The system of Claim 198 wherein: **(a)** AGPW outputs constrain allowable operations; **(b)** suspension flags propagate across dependent actions; and **(c)** cross-domain constraints remain active during execution.

Claim 202. The system of Claim 198 wherein: **(a)** equilibrium detection identifies convergence; **(b)** oscillations are dampened through weight adjustments; and **(c)** stability thresholds determine execution-mode transitions.

Claim 203. The system of Claim 198 wherein: **(a)** runtime enforcement integrates lineage-aware constraints; **(b)** multi-party dependencies influence allowed actions; and **(c)** Trust Criteria govern constraint propagation.

Claim 204. The system of Claim 198 wherein: **(a)** runtime policy execution incorporates jurisdictional rules; **(b)** merges cross-border constraints; and **(c)** harmonizes actions according to UTM policy bundles.

Claim 205. The system of Claim 198 wherein: **(a)** runtime feedback loops incorporate safety, risk, and compliance metrics; **(b)** multi-horizon updates modify equilibrium paths; and **(c)** corrective actions trigger downstream recalculations.

Claim 206. The system of Claim 198 wherein: **(a)** AGPW-guided execution determines which entities may act; **(b)** restricts actions inconsistent with global policy weights; and **(c)** enforces Trust Criteria across dependent workflows.

Claim 207. The system of Claim 198 wherein: **(a)** equilibrium is recalculated on governance updates; **(b)** runtime execution adapts without revealing underlying data; and **(c)** privacy-preserving feedback maintains compliance trajectories.

Claim 208. The system of Claim 198 wherein: **(a)** stable governance outcomes are enforced through weighted constraints; **(b)** unsatisfied policy conditions suspend execution; and **(c)** Trust Block updates reinstate or alter eligible actions.

Claim 209. The system of Claim 198 wherein: **(a)** AGPW outputs feed into tokenized value flows; **(b)** reweight allocations based on compliance and governance; and **(c)** govern incentive alignment across Exchange Networks.

Claim 210. The system of Claim 198 wherein: **(a)** runtime policy execution produces governance-derived Trust Blocks; **(b)** embeds updated weight vectors; and **(c)** propagates equilibrium outcomes to all dependent processes.

GROUP 7 — PRIVACY-PRESERVING PROCESS OPTIMIZATION SYSTEM (PPOS) (Claims 211-255)

The Privacy-Preserving Process Optimization System (PPOS) is the adaptive coordination and optimization fabric of the QPX ecosystem. While QPCs provide secure execution boundaries, Trust Blocks provide lineage, QRS provides trust scoring, and AGPW provides governance weightings, PPOS is the mechanism that translates these signals into optimized, rights-compliant, multi-party workflows. It does so without exposing personal data, proprietary information, or sensitive internal logic to counterparties or intermediaries.

PPOS solves a fundamental problem that plagues nearly every regulated domain: How can multiple entities—often with conflicting objectives, diverse constraints, and asymmetric access to information—coordinate and optimize shared processes without violating privacy or regulatory requirements? Traditional solutions require direct data sharing, enterprise integrations, bilateral agreements, or centralized oversight, all of which introduce risk, complexity, and friction. PPOS replaces these brittle architectures with a cryptographic, trust-verified optimization layer embedded in QPCs themselves.

At the core of PPOS is a privacy-preserving negotiation engine that evaluates multi-objective constraints—legal rules, contractual obligations, resource limits, fairness requirements, service-level expectations, and participant preferences—within Privacy Domains. The system computes a lawful, globally optimal outcome without disclosing any sensitive details. Participants do not need to expose internal decision models, users do

not reveal personal attributes, and enterprises do not expose proprietary rules or risk models. The QPC enforces both sides' constraints safely and optimally.

PPOS also governs fallback paths, exceptions, and dynamic constraint resolution. It ensures that a workflow can continue even if a participant withdraws, a QPC becomes ineligible, a constraint becomes unsatisfiable, or a regulatory condition changes mid-process. It accomplishes this through real-time re-optimization, dynamic rerouting, and safe substitution, all governed by AGPW, QRS, and Trust Blocks. This provides a robust, fault-tolerant architecture for high-stakes workflows across healthcare, finance, public services, logistics, and AI-agent coordination.

Finally, PPOS ensures that all workflow decisions are supported by verifiable lineage and Trust Blocks. Every optimization step, constraint evaluation, fallback decision, or substitution is cryptographically recorded—enabling full accountability, auditability, regulatory compliance, and downstream attribution. It transforms fragmented, opaque processes into verifiable workflows that remain private, lawful, and efficient.

Family 7.1 — Cryptographically Protected Negotiation & Multi-Objective Optimization

Establishes the cryptographic negotiation mechanism that allows multiple parties to converge on an optimal outcome without revealing sensitive information. Each participant's constraints, preferences, rights, and obligations are evaluated inside their QPC. Instead of exchanging data, QPCs exchange privacy-preserving optimization signals, enabling a distributed negotiation process in which no party sees another's private details. The result is a jointly optimized outcome that respects all applicable constraints while preserving strict confidentiality.

Converts negotiation—from clinical care pathways to financial underwriting to resource allocation to eligibility determinations—into a cryptographically mediated, trust-verified computation. Enterprises retain control over proprietary decision logic; users retain control over their personal rights and consent; and workflows become efficient, adaptive, and compliant. Because QPCs enforce Trust Criteria and AGPW policy weightings, the negotiation is always lawful, fair, and aligned with global governance requirements.

This enables privacy-preserving optimization across multiple parties—something demanded by nearly every regulated industry. Hospitals negotiating care pathways, insurers evaluating claims, financial institutions evaluating risk, public agencies coordinating benefits, logistics firms optimizing routes, or AI systems negotiating actions all require this mechanism. The claims effectively cover the foundational architecture for multi-party optimization under privacy constraints.

Claim 211. A system comprising, in any operable combination, one or more of:

(a) executing privacy-preserving multi-objective optimization;
(b) performing cryptographically protected negotiation across participants;
(c) aggregating constraint-bounded proposals; and

(d) selecting outcome vectors through encrypted scoring logic.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells; (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 212. The system of Claim 211 wherein: **(a)** encrypted negotiation masks party identities; **(b)** preserves policy constraints; and **(c)** exchanges only Trust-Block-derived signals during optimization.

Claim 213. The system of Claim 211 wherein: **(a)** multi-objective functions incorporate trust, compliance, cost, and risk metrics; **(b)** optimization weights derive from lineage attributes; and **(c)** outcomes reflect constraint-satisfying feasible sets.

Claim 214. The system of Claim 211 wherein: **(a)** encrypted negotiation rounds converge iteratively; **(b)** infeasible proposals are pruned; and **(c)** Trust Criteria restrict permissible negotiation pathways.

Claim 215. The system of Claim 211 wherein: **(a)** objective functions incorporate multi-party obligations; **(b)** policy-compliant action sets constrain optimization; and **(c)** outputs encode the resulting multi-objective solution vector.

Claim 216. The system of Claim 211 wherein: **(a)** negotiation messages are end-to-end encrypted; **(b)** contain only aggregated metrics; and **(c)** exclude underlying contractual or personal data.

Claim 217. The system of Claim 211 wherein: **(a)** scoring logic uses privacy-preserving computation; **(b)** computes comparative feasibility; and **(c)** selects weighted solutions under Trust Criteria constraints.

Claim 218. The system of Claim 211 wherein: **(a)** negotiation integrates cross-domain constraints; **(b)** harmonizes domain-specific limitations; and **(c)** generates a unified feasibility region.

Claim 219. The system of Claim 211 wherein: **(a)** infeasible negotiation proposals trigger fallback reductions; **(b)** trust-weighted penalties adjust scoring functions; and **(c)** solution vectors are recomputed accordingly.

Claim 220. The system of Claim 211 wherein: **(a)** negotiation constraints incorporate PBDR-related requirements; **(b)** benefit-distribution limits modify feasible outcomes; and **(c)** public-benefit obligations influence optimization paths.

Claim 221. The system of Claim 211 wherein: **(a)** multi-party negotiation runs asynchronously; **(b)** partial solutions are aggregated; and **(c)** scoring updates propagate upon new Trust Block evidence.

Claim 222. The system of Claim 211 wherein: **(a)** optimization incorporates domain-specific scoring functions; **(b)** aligns cross-domain constraints; and **(c)** selects solutions consistent with all mapped obligations.

Claim 223. The system of Claim 211 wherein: **(a)** negotiation includes trust-weighted contributions; **(b)** monitors constraint drift; and **(c)** ensures solution outputs remain policy-aligned.

Claim 224. The system of Claim 211 wherein: **(a)** encrypted negotiation incorporates semantic descriptors; **(b)** maps descriptors to constraint classes; and **(c)** adjusts optimization according to descriptor lineage.

Claim 225. The system of Claim 211 wherein: **(a)** optimization uses cross-party minimization of conflict signals; **(b)** Trust Criteria limit permissible negotiation sequences; and **(c)** resolution occurs through weighted feasible-set selection.

Claim 226. The system of Claim 211 wherein: **(a)** fallback objectives are triggered upon constraint violation; **(b)** reduced objective functions remain encrypted; and **(c)** optimization re-runs under stricter limits.

Claim 227. The system of Claim 211 wherein: **(a)** the final optimized output is encoded as a Trust Block; **(b)** embedded with constraint lineage; and **(c)** propagated to dependent processes for execution.

Family 7.2 — Contractual Routing, Constraint Satisfaction & Fallback

Extends PPOS by defining how contractual obligations, legal requirements, jurisdictional rules, and operational constraints are enforced through automated routing and fallback mechanisms. When a workflow encounters a constraint—such as an ineligible participant, a revoked consent, an updated policy requirement, or an unavailable resource—the QPC automatically computes alternative routes that preserve legal, ethical, and contractual compliance.

This formalizes the "self-healing workflow" paradigm within the QPX ecosystem. Instead of workflows breaking or defaulting into failure states, PPOS computes valid alternatives in real time, ensuring continuity without violating privacy or governance requirements. Fallback decisions are governed by lineage, Trust Criteria, AGPW weighting, and resource availability. The system ensures that workflows never operate outside their permissible bounds, and that all fallback decisions are fully auditable through Trust Blocks. Applies in industries where workflows must operate reliably under uncertainty—healthcare, insurance, financial services, public services, supply chain, and AI orchestration.

Claim 228. A system comprising, in any operable combination, one or more of:

(a) **performing contractual routing** using encrypted constraints;
(b) **selecting feasible contractual paths**;
(c) **applying fallback chains when obligations cannot be satisfied**; and
(d) **preserving privacy during contract-bound execution**.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells; (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 229. The system of Claim 228 wherein: **(a)** routing constraints incorporate contractual lineage; **(b)** policy dependencies shape allowable paths; and **(c)** conflict signals trigger fallback conditions.

Claim 230. The system of Claim 228 wherein: **(a)** routing logic computes trust-weighted segments; **(b)** infeasible constraints are pruned; and **(c)** contractual requirements govern path prioritization.

Claim 231. The system of Claim 228 wherein: **(a)** encrypted constraint satisfaction is executed iteratively; **(b)** verifying compliance without revealing underlying terms; and **(c)** mapping allowable actions to feasible execution sets.

Claim 232. The system of Claim 228 wherein: **(a)** multi-party contract terms are represented as constraint graphs; **(b)** dependences propagate across nodes; and **(c)** fallback paths activate upon violation detection.

Claim 233. The system of Claim 228 wherein: **(a)** fallback sequences are trust-weighted; **(b)** substitute participants inherit constraint lineage; and **(c)** Trust Criteria enforce compatibility limits.

Claim 234. The system of Claim 228 wherein: **(a)** routing uses semantic descriptors to classify obligations; **(b)** maps descriptors to constraint classes; and **(c)** maintains privacy for all underlying terms.

Claim 235. The system of Claim 228 wherein: **(a)** routing integrates jurisdiction-specific requirements; **(b)** cross-domain conflicts are resolved; and **(c)** fallback paths satisfy the most restrictive obligations.

Claim 236. The system of Claim 228 wherein: **(a)** encrypted constraint satisfaction includes risk-weighted scoring; **(b)** failure conditions adjust viability thresholds; and **(c)** fallback execution is triggered automatically.

Claim 237. The system of Claim 228 wherein: **(a)** fallback chains include multi-party substitutions; **(b)** substitute actors carry forward contractual lineage; and **(c)** Trust Criteria enforce their participation limits.

Claim 238. The system of Claim 228 wherein: **(a)** fallback pathways are re-evaluated as Trust Block evidence updates; **(b)** contract graph states adjust; and **(c)** routing recomputes feasible sets accordingly.

Claim 239. The system of Claim 228 wherein: **(a)** fallback outcomes incorporate public-benefit constraints; **(b)** lineage mapping detects restricted allocations; and **(c)** fallback paths trigger redistributive conditions as required.

Claim 240. The system of Claim 228 wherein: **(a)** routing computation integrates contribution-based metrics; **(b)** contract feasibility is adjusted by network-derived trust; and **(c)** fallback ordering incorporates trust-weighted priority.

Claim 241. The system of Claim 228 wherein: **(a)** encrypted routing logic runs asynchronously; **(b)** contract graph updates propagate dynamically; and **(c)** fallback computation recalibrates continuously.

Claim 242. The system of Claim 228 wherein: **(a)** final contractual routing outcomes generate Trust Blocks; **(b)** embed fallback lineage; and **(c)** propagate constraint satisfaction states to downstream processes.

Family 7.3 — Jurisdiction-Aware, Resource-Aware Matching & Execution

Defines the intelligent matching, execution, and fulfillment system that routes actions, requests, and resources to the appropriate entities based on jurisdictional rules, Trust Criteria, resource constraints, and dynamic eligibility. Unlike traditional matching systems that require centralized brokers or oversight, PPOS performs matching through distributed QPC computation, ensuring that neither the requester nor the provider reveals sensitive details that would normally be required for matching.

The system evaluates each participant's eligibility, obligations, risk posture, and jurisdictional constraints before determining whether a match is permissible. Once a match is established, PPOS ensures that execution routes comply with all contractual, regulatory, and governance constraints. If conditions change mid-execution—resource availability, consent revocation, jurisdictional updates—the system recalibrates and reroutes accordingly. This governs the matching layer that enables regulated markets and cross-domain workflows to function under privacy constraints.

Claim 243. A system comprising, in any operable combination, one or more of:

(a) performing jurisdiction-aware matching;

(b) selecting feasible actors, resources, and workflows;

(c) enforcing cross-jurisdiction constraints; and

(d) executing privacy-preserving, resource-aware process flows.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 244. The system of Claim 243 wherein: **(a)** jurisdiction-specific rules constrain matching; **(b)** cross-border limitations adjust resource selection; and **(c)** Trust Criteria determine permissible execution paths.

Claim 245. The system of Claim 243 wherein: **(a)** matching incorporates lineage-aware resource attributes; **(b)** policy bundles influence execution feasibility; and **(c)** semantic descriptors classify required capabilities.

Claim 246. The system of Claim 243 wherein: **(a)** resource-aware selection identifies compatible actors; **(b)** excludes constrained or suspended participants; and **(c)** computes feasible candidate sets.

Claim 247. The system of Claim 243 wherein: **(a)** jurisdiction-aware resolution harmonizes conflicting rules; **(b)** computes compliant execution paths; and **(c)** restricts actions violating any jurisdictional prerequisite.

Claim 248. The system of Claim 243 wherein: **(a)** execution integrates contract, policy, and jurisdictional obligations; **(b)** enforces constraint propagation; and **(c)** triggers fallback actions when required.

Claim 249. The system of Claim 243 wherein: **(a)** matching includes resource capacity constraints; **(b)** detects resource exhaustion; and **(c)** reroutes execution based on available capacity.

Claim 250. The system of Claim 243 wherein: **(a)** jurisdiction-aware matching incorporates risk and compliance metrics; **(b)** adjusts routing based on jurisdictional severity; and **(c)** applies weightings derived from Trust Blocks.

Claim 251. The system of Claim 243 wherein: **(a)** execution pathways are recalculated in real time; **(b)** Trust Block updates trigger re-matching; and **(c)** cross-domain constraints propagate dynamically.

Claim 252. The system of Claim 243 wherein: **(a)** resource-aware matching incorporates contribution metrics; **(b)** capability lineage influences feasibility; and **(c)** matching outputs reflect trust-weighted priority.

Claim 253. The system of Claim 243 wherein: **(a)** execution includes task decomposition; **(b)** assigns subtasks to feasible actors; and **(c)** recomposes results under policy constraints.

Claim 254. The system of Claim 243 wherein: **(a)** jurisdiction-aware resolution incorporates semantic descriptor mappings; **(b)** resolves descriptor conflicts; and **(c)** maintains descriptor lineage throughout execution.

Claim 255. The system of Claim 243 wherein: **(a)** final execution results generate Trust Blocks; **(b)** embed jurisdictional and resource lineage; and **(c)** distribute execution metadata to downstream systems.

GROUP 8 — EXCHANGE NETWORKS, RESOURCE POOLS & TRUST-VERIFIED TOKENIZATION (Claims 256-305)

Defines the economic coordination layer of the Quantum Privacy Exchange (QPX). While previous Groups established QPCs, Trust Blocks, PoT lineage, Trust Criteria, QRS ratings, AGPW governance, and PPOS optimization, Group 8 introduces the **tokenization and settlement infrastructure** that enables privacy-preserving, trust-verified exchange of resources, services, obligations, and computational outcomes across the network.

Solves one of the most persistent structural challenges of digital ecosystems: how to represent rights, value, entitlements, and obligations in a manner that is privacy-preserving, cryptographically verifiable, and dynamically governed. Rather than treating tokens as financial instruments or blockchain artifacts, QPX tokens serve as **governed representations of rights and obligations** whose lifecycle, usage constraints, provenance, and eligibility are enforced inside QPCs through Trust Criteria. Every token in QPX is embedded with lineage metadata and execution constraints, ensuring that it may only be redeemed, transferred, or exercised under compliant & policy-aligned conditions.

Group 8 also defines the architecture of **Exchange Networks**, which match and clear tokenized requests, obligations, or resources through trust-verified workflows. These networks operate without revealing identity, proprietary data, or sensitive internal states of participants. Every transaction occurs through Privacy Domains, and every clearing operation is validated through PoT, Trust Blocks, and QRS ratings.

The final pillar of Group 8 is **Multi-Pool Coordination and Liquidity Routing**, which ensures that Resource Pools, Token Pools, and Liquidity Pools operate safely and efficiently at population scale. These pools preserve privacy while allowing dynamic reallocation, fallback resolution, multi-hop execution, and cross-domain optimization. Combined, these mechanisms allow QPX to function as a **universal, privacy-preserving exchange layer** that supports markets for regulated services, personalized experiences, AI-agent capabilities, public-benefit incentives, and complex multi-party workflows.

Family 8.1 — Resource Tokens & Provenance-Governed Allocation

Resource Tokens represent governed rights, entitlements, obligations, or quantized resource allocations within the QPX ecosystem. These tokens are not financial commodities; they are privacy-preserving wrappers around a defined capability or resource that may only be redeemed or exercised under Trust Criteria enforced by a QPC. Every token is embedded with detailed provenance metadata—including the originating authority, contractual terms, jurisdictional conditions, and consent lineage—and these details remain private while still being cryptographically verifiable.

The system ensures that Resource Tokens may only be exercised when all constraints are satisfied. QPCs evaluate eligibility using Trust Blocks, PoT attestations, and QRS ratings. If a participant's trust posture changes, or if governance rules evolve through AGPW, tokens dynamically update their permissible usage conditions. This fully decouples entitlement management from enterprise identity systems and eliminates the need for centralized credentialing databases or manual verification steps.

This defines the mechanism for representing **regulated rights and entitlements** in a privacy-preserving, trust-verifiable manner. Healthcare benefits, financial eligibility, service entitlements, compliance obligations, public-benefit allocations, subscription rights, AI capabilities, and enterprise permissions can all be expressed as Resource Tokens. This creates a universal entitlement infrastructure that enterprises, governments, and AI platforms will require to operate lawfully and efficiently in a privacy-first world.

Claim 256. A system comprising, in any operable combination, one or more of:

(a) a **Resource Token** representing a cryptographically bound set of provenance attributes, usage rights, and allocation constraints;
(b) a **Trust Block** encoding lineage, custodial relationships, and inherited Trust Criteria for the Resource Token;
(c) a **Resource Pool** maintaining multiple Resource Tokens with synchronized provenance metadata;
(d) a **policy-evaluation module** that validates each token's request for use against provenance-governed allocation rules;
(e) a **rights-enforcement layer** that redeems or activates a Resource Token only when its provenance lineage satisfies all applicable constraints;
(f) a **metadata inheritance engine** that attaches upstream Trust Criteria to all derivative assets formed from the Resource Token.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells; (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 257. A system comprising, in any operable combination, one or more of:

(a) a Resource Token issuance service that converts a provider-controlled resource into a tokenized representation;
(b) a provenance-governed rights model specifying permissible transformations of the resource;
(c) a Trust Block chain recording each transfer, reuse, or combination event;
(d) a validator that halts redemption upon detecting unmet provenance constraints;
(e) a decision engine that approves derivative formation only when all upstream obligations remain preserved.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 258. A system comprising, in any operable combination, one or more of:

(a) a mechanism that groups Resource Tokens into Resource Pools based on shared provenance or contractual lineage;
(b) a pool-governance module that enforces allocation priority rules for each Resource Token;
(c) a discovery service enabling participants to request rights governed by those tokens;
(d) a cryptographic check that rejects requests when the requester's Trust Block evidence does not satisfy inherited provenance requirements.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 259. A system comprising, in any operable combination, one or more of:

(a) a Resource Token configured to encode origin-provider metadata, permissible usage contexts, and revocation policies;
(b) a dynamic update mechanism that appends new provenance conditions upon downstream reuse;
(c) a validator that recomputes eligibility at each activation event;
(d) an automated revocation mechanism triggered by failure to satisfy lineage-bound constraints;
(e) a ledger of Trust Blocks documenting each change of state.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 260. A system comprising, in any operable combination, one or more of:

(a) Resource Tokens that embed contractual and jurisdictional restrictions inherited from multiple upstream providers;
(b) a rule compiler that merges these inherited obligations into enforceable allocation criteria;
(c) a token-usage engine that executes or denies operations based on compiled lineage rules;
(d) a provenance-hash service that binds all inherited constraints to a non-repudiable Trust Block.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 261. A system comprising, in any operable combination, one or more of:

(a) Resource Tokens whose permissible conversions, combinations, or redemptions depend on multi-party provenance inputs;
(b) a consensus engine that evaluates these inputs using aggregated Trust Criteria;
(c) a rights allocator that distributes resource entitlements based on consensus-approved lineage;
(d) an enforcement module that prevents violations of co-owner or co-originator restrictions.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 262. A system comprising, in any operable combination, one or more of:

(a) a Resource Pool composed of tokens representing data, content, compute, workflows, or other QPN-governed resources;
(b) a pool-allocation engine that determines token distribution based on provenance-governed priority;
(c) an eligibility module that computes requester rights from their Trust Blocks;
(d) an enforcement layer that adjusts allocation outcomes according to lineage conditions of each token.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 263. A system comprising, in any operable combination, one or more of:

(a) a merging engine that aggregates multiple Resource Tokens into a composite derivative token;
(b) a lineage-preservation module that binds aggregated constraints into a unified provenance profile;
(c) a validator that ensures derivative use cannot violate any upstream rules;
(d) a recombination service that forms new Resource Pools from derivative tokens.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 264. A system comprising, in any operable combination, one or more of:

(a) a mechanism for subdividing a Resource Token into fractional entitlements;
(b) a lineage-splitting algorithm that propagates provenance constraints proportionally to each fragment;
(c) a redemption check requiring each fragment's requester to independently satisfy lineage obligations;
(d) a settlement engine that recombines fragments only upon compliance with all upstream Trust Criteria.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 265. A system comprising, in any operable combination, one or more of:

(a) Resource Tokens that encode expiration, decay, or renewal conditions inherited from upstream provenance;
(b) a lifecycle engine that adjusts token state based on usage events;
(c) a validity-check module that rejects expired lineage rights;
(d) a renewal mechanism requiring updated Trust Block evidence before extension.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 266. A system comprising, in any operable combination, one or more of:

(a) Resource Tokens that encode multi-stakeholder benefit-allocation rules;
(b) a provenance-governed revenue-sharing engine;
(c) a ledger of Trust Blocks documenting each entitlement path;
(d) an enforcement layer that ensures allocations correspond to lineage-derived percentages.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 267. A system comprising, in any operable combination, one or more of:

(a) Resource Tokens that embed consent lineage inherited from PPN or EPN domain rules;
(b) a consent-propagation engine that merges individual or enterprise-defined restrictions;
(c) a resolver that validates token use against all upstream consent-derived obligations;
(d) a disallow mechanism that prevents use when any consent lineage is violated.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 268. A system comprising, in any operable combination, one or more of:

(a) a Resource Token configured to bind financial, legal, and jurisdictional constraints to a single cryptographic object;
(b) a lineage-check engine that verifies multi-jurisdiction compliance;
(c) a settlement filter that prevents allocation when aggregated lineage violates any jurisdictional rule;
(d) a cross-domain Trust Block record of all validation steps.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 269. A system comprising, in any operable combination, one or more of:

(a) Resource Tokens that describe allowed downstream commercial uses;

(b) a policy-translation engine that maps commercial restrictions into executable Trust Criteria;

(c) a usage-evaluation module that enforces these restrictions during allocation;

(d) a provenance record that identifies all commercial contexts in which the Resource Token may be used.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 270. A system comprising, in any operable combination, one or more of:

(a) Resource Tokens that encode required minimum Trust Ratings for reuse;

(b) a rating-evaluation engine that checks the requester's Trust Block metrics;

(c) an eligibility gate that denies reuse when the requester's rating does not satisfy token-specific thresholds;

(d) a ledger update indicating the rating criteria applied.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 271. A system comprising, in any operable combination, one or more of:

(a) Resource Tokens representing rights that must be redeemed through a QPN-governed workflow;

(b) a workflow-binding module that maps redemption to required tasks;

(c) a validator ensuring each task meets lineage-derived restrictions;

(d) a finalization service that issues a settlement Trust Block upon completion.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 272. A system comprising, in any operable combination, one or more of:

(a) Resource Tokens that encode substitution policies permitting replacement resources;

(b) a provenance-match engine that identifies allowable substitutes;

(c) a constraint-check system ensuring substitute resources satisfy all inherited obligations;

(d) a substitution Trust Block documenting the authorized replacement.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 273. A system comprising, in any operable combination, one or more of:

(a) Resource Tokens representing tiered access rights;
(b) a tier-evaluation mechanism that determines allowable rights based on lineage and requester Trust Criteria;
(c) a rights-enforcement module preventing elevation beyond lineage constraints;
(d) a record of all permitted tiers encoded in Trust Blocks.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 274. A system comprising, in any operable combination, one or more of:

(a) Resource Tokens describing upstream ownership splits;
(b) a rights-apportionment engine enforcing provenance-governed benefit allocation;
(c) a validator ensuring apportionment remains consistent through all derivative formations;
(d) a settlement record documenting each apportionment event.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 275. A system comprising, in any operable combination, one or more of:

(a) Resource Tokens that encode mandatory auditability conditions;
(b) a provenance-check engine that verifies lineage completeness prior to redemption;
(c) a denial mechanism for tokens lacking sufficient Trust Block evidence;
(d) an audit Trust Block documenting the validation event.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Family 8.2 — Exchange Networks & Trust-Verified Clearing

Defines the architecture of the **Exchange Networks** that match, route, and clear Resource Tokens, Solution Tokens, obligations, requests, and rights across the QPX ecosystem. Unlike traditional exchanges that require identity disclosure or centralized clearing authorities, QPX exchanges operate entirely within Privacy Domains. Every transaction is validated through PoT attestations and Trust Blocks, ensuring that counterparties remain

anonymous while still cryptographically verifying eligibility, compliance, and the validity of the underlying token.

These Exchange Networks enable complex value flows without any party revealing sensitive information. The network evaluates jurisdictional rules, risk profiles, resource constraints, QRS trust ratings, and AGPW policy weightings to determine whether a given match or clearing operation is lawful and permissible. Once validated, the system routes settlement instructions through QPC-governed workflows, ensuring that value transfer is fully traceable and auditable without revealing identity or data.

This provides a central licensing lever, as it governs the operation of **trust-verified exchanges** that serve as the backbone of QPX. Healthcare networks, financial services platforms, supply chain consortia, enterprise marketplaces, government benefits programs, and AI ecosystems will require Exchange Network capabilities to operate safely and lawfully. These claims will be indispensable for any market operator seeking privacy-preserving, automated, compliance-aware clearing mechanisms.

Claim 276. A system comprising, in any operable combination, one or more of:

(a) an **Exchange Network** linking multiple **Resource Pools**;
(b) a **routing engine** that identifies candidate exchanges between participants;
(c) a **Trust-Verified Clearing module** that validates each proposed exchange using PoT-derived Trust Blocks;
(d) a **settlement engine** that finalizes exchanges only when all lineage obligations remain satisfied.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 277. A system comprising, in any operable combination, one or more of:

(a) an **Exchange Network** configured to match buyer and seller requests using privacy-preserving Trust Criteria;
(b) a **matching engine** that computes compatibility without revealing identities;
(c) a **clearing engine** verifying satisfaction of provenance and compliance obligations;
(d) a **settlement recorder** generating a Trust Block representing the completed exchange.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 278. A system comprising, in any operable combination, one or more of:

(a) an **Exchange Network** that performs trust-weighted matching of Resource Tokens;

(b) a **pricing engine** that adjusts exchange value using Trust Ratings derived from Trust Blocks;

(c) a **settlement layer** that enforces lineage and constraint checks;

(d) a **proof generator** issuing a settlement Trust Block.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 279. A system comprising, in any operable combination, one or more of:

(a) an **Exchange Network** configured for multi-party clearing;

(b) a **compatibility engine** evaluating Trust Criteria for all parties;

(c) a **privacy-preserving clearing protocol** that ensures compatibility without identity disclosure;

(d) a **settlement Trust Block** representing the verified multi-party exchange.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 280. A system comprising, in any operable combination, one or more of:

(a) an **Exchange Network** that supports batch-clearing of multiple Resource Tokens;

(b) a **batching engine** that aggregates compatible requests;

(c) a **Trust-Verified Clearing mechanism** that validates aggregated lineage;

(d) a **unified settlement Trust Block** documenting the batch-clearing event.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 281. A system comprising, in any operable combination, one or more of:

(a) an **Exchange Network** capable of anonymous counterparty discovery;

(b) a **privacy-preserving matching protocol** evaluating Trust Criteria without disclosing identities;

(c) a **clearing module** enforcing lineage compliance;

(d) a **settlement engine** validating exchange correctness before issuing a settlement Trust Block.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 282. A system comprising, in any operable combination, one or more of:

(a) an **Exchange Network** supporting sequential clearing across multiple pools;

(b) a **dependency-engine** evaluating lineage constraints that span pools;

(c) a **clearing sequencer** that enforces required ordering of validation steps;

(d) a **Trust Block** documenting cross-pool clearing provenance.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 283. A system comprising, in any operable combination, one or more of:

(a) an **Exchange Network** that executes conditional clearing operations;
(b) a **condition-resolution module** interpreting lineage prerequisites;
(c) a **clearing engine** performing multi-step validation;
(d) a **conditional settlement** record captured as a Trust Block.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 284. A system comprising, in any operable combination, one or more of:

(a) an **Exchange Network** offering moderated or permissioned exchange participation;
(b) a **permission-check module** evaluating Trust Blocks;
(c) a **clearing mechanism** enforcing moderator-defined constraints;
(d) a **settlement audit record** appended as a Trust Block.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 285. A system comprising, in any operable combination, one or more of:

(a) an **Exchange Network** evaluating bilateral or multilateral Trust Ratings;
(b) a **compatibility engine** determining exchange viability based on rating thresholds;
(c) a **clearing module** that denies settlement for incompatible ratings;
(d) a **settlement Trust Block** documenting applied thresholds.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 286. A system comprising, in any operable combination, one or more of:

(a) an **Exchange Network** performing automated discovery of substitute counterparties;
(b) a **lineage-match engine** identifying valid substitutes;
(c) a **clearing module** ensuring substitute exchanges satisfy all provenance obligations;
(d) a **settlement Trust Block** documenting substitute clearing.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 287. A system comprising, in any operable combination, one or more of:

(a) an **Exchange Network** that supports asynchronous clearing events;
(b) a **stateful clearing engine** tracking lineage constraints across time;
(c) a **validation step** that ensures lineage remains satisfied at each asynchronous stage;
(d) a **final settlement** Trust Block documenting completion.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 288. A system comprising, in any operable combination, one or more of:

(a) an **Exchange Network** performing zero-knowledge clearing;
(b) a **cryptographic proof engine** validating Trust Criteria without revealing underlying information;
(c) a **settlement mechanism** triggered only upon verified satisfaction;
(d) a **Trust Block** recording the zero-knowledge clearing result.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 289. A system comprising, in any operable combination, one or more of:

(a) an **Exchange Network** performing simultaneous matching across multiple asset classes;
(b) a **constraint solver** verifying lineage compatibility across classes;
(c) a **clearing module** validating multi-asset settlement;
(d) a **unified settlement Trust Block** documenting the matched exchange. EasyAccess workflow threads.

Claim 290. A system comprising, in any operable combination, one or more of:

(a) an **Exchange Network** that uses Trust Block-derived compliance rules to determine allowable exchange paths;
(b) a **rule-evaluation engine** that selects a valid clearing path;
(c) a **settlement engine** that executes the selected path;
(d) a **settlement Trust Block** documenting the rule-based exchange path.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Family 8.3 — Multi-Pool Coordination & Liquidity Routing

Introduces the infrastructure for **Resource Pools, Token Pools, and Liquidity Pools**, which provide collective mechanisms for allocation, matching, fallback, rebalancing, and multi-hop routing. In traditional systems, liquidity management and resource allocation require direct data sharing, centralized oversight, or cross-party visibility. QPX replaces these models with **privacy-preserving multi-pool mechanisms** where each pool is governed by QPC-enforced Trust Criteria.

The system evaluates resource availability, trust posture, risk, AGPW weighting, and cross-domain dependencies to determine how resources should be allocated or routed. When conditions change—such as resource depletion, policy updates, or eligibility shifts—the system automatically rebalances pools and routes requests to maintain system-level resilience. Multi-hop routing enables requests to cross pools and jurisdictions while preserving privacy and lineage integrity. This ensures that large-scale ecosystems can operate efficiently even under dynamic and uncertain conditions.

This supports **pool-based resource coordination**, which is essential to nearly every regulated, large-scale digital ecosystem. Healthcare capacity allocation, government benefits distribution, financial liquidity management, supply chain rebalancing, and AI resource orchestration all depend on privacy-preserving, trust-verified pooling mechanisms.

Claim 291. A system comprising, in any operable combination, one or more of:

(a) a plurality of **Resource Pools**, **Token Pools**, and **Liquidity Pools**;
(b) a **routing engine** that identifies optimal paths across pools;
(c) a **Trust Criteria evaluator** ensuring all routing steps satisfy lineage and compliance constraints;
(d) a **cross-pool settlement module** issuing a unified settlement Trust Block.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 292. A system comprising, in any operable combination, one or more of:

(a) a **liquidity-routing engine** that determines amounts to draw from multiple Liquidity Pools;
(b) a **trust-weight calculation** determining allowable liquidity sources;
(c) a **compliance filter** enforcing lineage constraints;
(d) a **settlement record** encoded as a Trust Block.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 293. A system comprising, in any operable combination, one or more of:

(a) a **coordination engine** that synchronizes Resource Pools with Exchange Networks;
(b) a **multi-pool evaluation module** assessing compatibility of pooled resources;
(c) a **routing module** that selects viable resource paths;
(d) a **settlement log** encoded in a Trust Block.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 294. A system comprising, in any operable combination, one or more of:
(a) a **fallback-routing mechanism** that identifies substitute pools when a preferred route fails;
(b) a **lineage-check engine** ensuring substitute pools satisfy all constraints;
(c) a **routing selector** assigning a new path;
(d) a **Trust Block** documenting the fallback event.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 295 A system comprising, in any operable combination, one or more of:
(a) Liquidity Pools whose routing eligibility depends on Trust Ratings;
(b) a **rating-evaluator** determining allowable liquidity contributors;
(c) a **routing engine** that selects liquidity sources based on these ratings;
(d) a **settlement Trust Block** documenting rating-based routing.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 296. A system comprising, in any operable combination, one or more of:
(a) Resource Pools that dynamically rebalance based on demand;
(b) a **rebalancing engine** evaluating Trust Criteria for each pool;
(c) a **routing module** reallocating resources accordingly;
(d) a **Trust Block** documenting rebalancing actions.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 297. A system comprising, in any operable combination, one or more of:
(a) a **cross-domain routing engine** linking Resource Pools across jurisdictions;
(b) a **compliance module** evaluating jurisdiction-specific constraints;
(c) a **routing filter** selecting compliant pools;
(d) a **Trust Block** documenting jurisdictional routing decisions.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 298. A system comprising, in any operable combination, one or more of:

(a) a **liquidity-coordination engine** that distributes liquidity demands across multiple pools;

(b) a **trust-governed weighting algorithm** determining distribution amounts;

(c) a **lineage-check system** ensuring each pool satisfies routing constraints;

(d) a **settlement Trust Block** documenting distribution results.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 299. A system comprising, in any operable combination, one or more of:

(a) Resource Pools with tiered-access levels;

(b) an **access-evaluator** determining which tiers are available to each requester;

(c) a **routing engine** selecting pool paths consistent with tier restrictions;

(d) a **Trust Block** encoding tier-based routing decisions.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 300. A system comprising, in any operable combination, one or more of:

(a) a **pool-compatibility analyzer** evaluating whether the combination of two Resource Pools satisfies aggregated lineage;

(b) a **routing engine** that permits combination only when compatible;

(c) a **settlement module** documenting combined-pool outcomes;

(d) a **Trust Block** representing compatibility verification.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 301. A system comprising, in any operable combination, one or more of:

(a) a predictive routing engine evaluating dynamic pool conditions;

(b) a trust-governed prediction model identifying optimal cross-pool routes;

(c) a lineage-check ensuring predicted routes remain compliant;

(d) a Trust Block recording prediction-based routing.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 302. A system comprising, in any operable combination, one or more of:

(a) a **cascading-routing mechanism** enabling chained cross-pool operations;

(b) a **lineage-validator** executed at each stage;
(c) a **constraint module** detecting violations mid-route;
(d) a **cascading-settlement Trust Block** documenting validated stages.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 303. A system comprising, in any operable combination, one or more of:
(a) a **liquidity-fallback engine** identifying replacement Liquidity Pools;
(b) a **compatibility module** confirming each substitute satisfies lineage;
(c) a **routing update** selecting the fallback source;
(d) a **Trust Block** documenting fallback liquidity routing.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 304. A system comprising, in any operable combination, one or more of:
(a) a **multi-pool optimization engine** computing exchange efficiency metrics;
(b) a **trust-weighted scoring module** determining optimal route selection;
(c) a **lineage-check** verifying compliance of the selected route;
(d) a **settlement Trust Block** documenting the optimized route.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 305. A system comprising, in any operable combination, one or more of:
(a) **Resource Pools, Token Pools**, and **Liquidity Pools** engaged in coordinated, trust-verified routing;
(b) a **unified routing engine** synchronizing cross-pool operations;
(c) a **compliance overlay** enforcing lineage, jurisdictional, and contractual constraints;
(d) a **consolidated settlement Trust Block** documenting all coordinated routing actions.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

GROUP 9 — AI AGENTS, MULTI-AGENT COORDINATION & FEDERATED DOMAIN GOVERNANCE (Claims 306–350)

Governs how AI agents operate inside the Quantum Privacy Network. While traditional AI systems function as opaque black boxes—often lacking verifiable lineage, rights enforcement, or reliable governance—QPN-based AI agents operate within QPC-enforced Privacy Domains with transparent, verifiable constraints. This transforms AI from an

uncontrolled computational actor into a trust-verified, policy-aligned, privacy-preserving participant whose behavior can be explained, audited, and governed.

Every AI agent can be anchored to its own QPC, which constrains perception, computation, and action. The QPC mediates all inputs and outputs, enforcing Trust Criteria, AGPW policy weightings, QRS capability ceilings, and contractual or jurisdictional constraints. This ensures that no AI agent can exceed its authorized scope, access sensitive data, invoke prohibited workflows, or take actions inconsistent with the rights or obligations of its operator.

A second pillar is the coordination of multiple AI agents—potentially acting on behalf of different participants, enterprises, or regulatory bodies—without exposing proprietary models or private data. QPN introduces privacy-preserving planning, multi-agent workflow alignment, and trust-verified delegation mechanisms that allow agents to collaborate safely. Through lineage-governed plans, PoT-backed validation steps, and entanglement metadata, multi-agent behavior becomes explainable, auditable, and controllable without requiring centralized oversight.

Group 9 defines the **federated governance model** where AI agents across different enterprises, jurisdictions, or domains do not rely on a single authority. Instead, governance emerges through federated policy signals supplied by Human-Managed Trust Authorities (HTAs) and harmonized through AGPW, ensuring AI behavior remains aligned with legal frameworks, cultural values, institutional norms, and ecological objectives while maintaining global interoperability. This enables a world where autonomous systems can act safely at scale—with privacy, trust, governance, and accountability woven directly into their operational fabric.

Family 9.1 — QPC-Governed AI Agents

Establishes the foundational model for AI agents operating within QPCs. AI agents become first-class participants in the trust ecosystem only when their computation is bounded by a QPC Privacy Domain. Inside this domain, all sensory inputs, internal states, learned representations, inference steps, model outputs, and external actions are mediated by Trust Criteria. This prevents the agent from accessing unapproved data, inferring protected attributes, engaging in harmful optimization, or violating contractual or regulatory restrictions.

The QPC also ensures that all AI actions carry lineage metadata, enabling complete traceability and auditability. Every inference step can be tied back to trust-verified models, datasets, and policies. Because all computation remains sealed inside a Privacy Domain, even powerful agents cannot circumvent governance or safety constraints. This establishes a new paradigm in which AI systems are both autonomous and inherently governable.

As AI becomes more capable, enterprises and regulators can require architectures that guarantee lawful, safe, and privacy-preserving operation. Any AI product that interacts with

users, enterprises, or regulated sectors will need QPC governance mechanisms to ensure safety and alignment – essential for AI labs, cloud providers, enterprises deploying AI co-pilots, and operators of autonomous agents.

Claim 306. A system comprising, in any operable combination, one or more of:

(a) an **AI agent** anchored to a **Quantum Privacy Cell** (QPC) that governs all perception, inference, planning, and action;

(b) a **Trust Criteria evaluation module** determining permissible behaviors for the agent;

(c) a **capability-ceiling engine** deriving agent limits from **Quantum Rating System** (QRS) and **Adaptive Global Policy Weighting** (AGPW) parameters;

(d) a **Proof-of-Trust (PoT) validator** authorizing or rejecting planned actions based on the agent's Trust Block lineage;

(e) a **privacy-bound routing module** ensuring all agent interactions occur within authorized Privacy Domains.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 307. A system comprising, in any operable combination, one or more of:

(a) a QPC-governed AI agent whose sensory inputs are restricted to QPC-approved data channels;

(b) an **inference engine** required to evaluate Trust Criteria before generating internal representations;

(c) a **planning module** constrained by AGPW-weighted policy parameters;

(d) an **action engine** that cannot execute an action unless PoT validation succeeds;

(e) a **Trust Block recorder** documenting all authorized agent states.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 308. A system comprising, in any operable combination, one or more of:

(a) a **QPC-bounded AI agent** with privacy-preserving access to domain-specific resources;

(b) a **dynamic Trust Criteria interpreter** mapping domain rules to behavioral constraints;

(c) a **capability-governor** adjusting permissible actions according to QRS-derived ceilings;

(d) a **PoT enforcement layer** preventing execution of disallowed actions;

(e) a **workflow dispatcher** binding agent outputs to authorized EasyAccess workflow threads.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 309. A system comprising, in any operable combination, one or more of:

(a) a **QPC-contained inference engine** performing trust-bounded reasoning;
(b) a **constraint-evaluation layer** that verifies compliance with AGPW policies;
(c) a **planner** generating alternative actions validated against Trust Criteria;
(d) an **executor** that performs actions only upon PoT confirmation;
(e) a **lineage tracker** encoding reasoning steps as Trust Blocks.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 310. A system comprising, in any operable combination, one or more of:

(a) an **AI agent** executing within a Privacy Domain that restricts external communication to approved channels;
(b) a **Trust Criteria evaluator** filtering all outbound messages;
(c) a **QRS-based capability limiter** preventing high-risk operations;
(d) a **PoT engine** certifying agent-generated outputs comply with domain rules;
(e) a **Trust Block log** documenting outbound communications.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 311. A system comprising, in any operable combination, one or more of:

(a) a QPC-governed agent that receives task prompts through authorized workflow threads;
(b) a Trust Criteria analyzer deriving permissible task paths;
(c) a planner that selects among Trust-Criteria-compliant plans;
(d) a PoT validator that confirms permitted plan execution;
(e) a lineage recorder encoding each planning decision in Trust Blocks.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 312. A system comprising, in any operable combination, one or more of:

(a) a **QPC-governed agent** maintaining an internal state subject to Trust Criteria;
(b) a **domain-policy translator** mapping AGPW policies to internal state constraints;
(c) a **state-transition engine** that validates transitions using PoT;
(d) an **enforcement module** preventing unauthorized state changes;
(e) a **Trust Block registry** recording validated transitions.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 313. A system comprising, in any operable combination, one or more of:

(a) a **QPC-bound perception module** that filters sensory inputs using Trust Criteria;

(b) a **reasoning module** constrained by QRS ceilings;

(c) a **planning layer** governed by AGPW policies;

(d) an **execution layer** requiring PoT approval;

(e) an **audit layer** encoding perception-to-action lineage in Trust Blocks.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 314. A system comprising, in any operable combination, one or more of:

(a) a **QPC-contained agent** that evaluates the trustworthiness of inputs based on upstream lineage;

(b) a **Trust Block analyzer** computing confidence weights;

(c) a **planning module** influenced by AGPW-weighted domain rules;

(d) a **PoT-restricted action engine**;

(e) a **Trust Block recorder** documenting trust-weighted decision-making.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 315. A system comprising, in any operable combination, one or more of:

(a) a **QPC-governed inference engine** that utilizes Trust Criteria to exclude impermissible reasoning paths;

(b) a **planning engine** applying AGPW-adjusted constraints;

(c) a **QRS-based decision filter**;

(d) an **action executor** governed by PoT;

(e) a **lineage-capture module** generating Trust Blocks for each validated reasoning chain.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 316. A system comprising, in any operable combination, one or more of:

(a) an **AI agent** whose model weights or parameters are bounded by QPC-governed policies;

(b) a **Trust Criteria gate** controlling updates to internal parameters;

(c) an **AGPW-based evaluator** determining whether parameter changes satisfy domain rules;

(d) a **PoT validator** certifying approved updates;
(e) a **Trust Block registry** encoding authorized modifications.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 317. A system comprising, in any operable combination, one or more of:
(a) a **QPC-governed agent** configured to participate in domain-specific workflows;
(b) a **workflow-policy engine** applying Trust Criteria to determine permissible workflow steps;
(c) an **AGPW-governed planner** selecting among compliant step sequences;
(d) a **PoT executor** authorizing step completion;
(e) a **Trust Block ledger** recording workflow participation.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 318. A system comprising, in any operable combination, one or more of:
(a) a **QPC-bound agent** that evaluates upstream Trust Blocks before accepting instructions;
(b) a **Trust Criteria evaluator** confirming instruction legitimacy;
(c) a **planning module** constrained by AGPW-derived rules;
(d) a **PoT-based execution engine**;
(e) an **instruction provenance recorder** generating downstream Trust Blocks.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Family 9.2 — Multi-Agent Plans & Safe Coordination

In real-world workflows—clinical decision support, financial compliance, supply chain coordination, autonomous vehicle swarms, multi-copilot enterprise environments—multiple AI agents must collaborate. Traditional architectures either require full data sharing (which violates privacy and IP boundaries) or rely on brittle, centralized coordination mechanisms.

QPC-governed AI agents can collaborate through privacy-preserving, lineage-anchored multi-agent plans. Each agent contributes constrained capabilities and only receives the information permitted by its Trust Criteria and AGPW-defined policy ceilings. Plans are decomposed into tasks that are allocated to agents based on trust posture, eligibility, jurisdiction, and resource considerations. Entanglement metadata ensures that changes in policy, capability, or eligibility propagate safely across the coordinated agent set.

This uniquely enables safe AI collaboration in applications with strict safety or privacy constraints – banks, hospitals, logistics operators, insurance carriers, defense systems, and enterprise AI copilots will require this architecture. Multi-agent alignment is a known

unsolved problem for the AI industry, and these claims provide a practical, governable solution that preserves IP boundaries while enabling autonomous coordination.

Claim 319. A system comprising, in any operable combination, one or more of:

(a) multiple QPC-governed AI agents participating in a shared workflow;
(b) an **inter-agent coordination engine** that evaluates Trust Criteria for all participants;
(c) an **AGPW-governed policy layer** determining multi-agent behavior limits;
(d) a **PoT-based verification module** confirming safe coordination steps;
(e) a **Trust Block ledger** recording multi-agent collaboration lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 320. A system comprising, in any operable combination, one or more of:

(a) a **multi-agent plan generator** constructing coordinated agent tasks;
(b) a **Trust Criteria evaluator** validating that interdependent actions comply with domain constraints;
(c) a **capability-governance engine** applying QRS ceilings to each agent;
(d) a **PoT clearing module** authorizing multi-agent plan execution;
(e) a **Trust Block sequence** encoding plan lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 321. A system comprising, in any operable combination, one or more of:

(a) a coordination fabric enabling privacy-preserving communication between QPC-governed agents;
(b) a Trust Criteria filter validating inter-agent message legitimacy;
(c) an AGPW-based policy interpreter adjusting collaboration permissions;
(d) a PoT-based approval engine validating each coordinated exchange;
(e) a Trust Block ledger documenting communication lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 322. A system comprising, in any operable combination, one or more of:

(a) a **multi-agent workflow scheduler** assigning tasks to agents based on Trust Criteria;
(b) a QRS**-governed capacity evaluator** determining allowable workload per agent;
(c) an **AGPW policy engine** coordinating cross-agent decisions;
(d) a **PoT-based scheduler validator** confirming safe task assignment;
(e) a **Trust Block record** documenting scheduling lineage.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 323. A system comprising, in any operable combination, one or more of:

(a) a **trust-bounded negotiation module** enabling safe coordination between agents;

(b) a **Trust Criteria engine** determining permissible negotiation outcomes;

(c) an **AGPW policy gate** preventing negotiation paths that exceed domain constraints;

(d) a **PoT clearing mechanism** validating negotiated results;

(e) a **Trust Block** log documenting negotiation lineage.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 324. A system comprising, in any operable combination, one or more of:

(a) a **conflict-resolution engine** for multi-agent workflows;

(b) a **Trust Criteria evaluator** identifying conflicting behaviors;

(c) an **AGPW-governed policy engine** resolving conflicts within established domain limits;

(d) a **PoT-authorized resolution executor**;

(e) a **Trust Block** documenting the conflict-resolution decision.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 325. A system comprising, in any operable combination, one or more of:

(a) a **shared-resource allocator** distributing resources among QPC-governed agents;

(b) a **Trust Criteria evaluator** determining allocation permissions;

(c) an **AGPW-influenced allocation policy**;

(d) a **PoT-based verification engine** approving allocations;

(e) a **Trust Block ledger** documenting resource distribution.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 326. A system comprising, in any operable combination, one or more of:

(a) a **multi-agent capability-balancing engine** preventing unsafe aggregation of agent capacities;

(b) a **QRS evaluator** determining safe combined capacity levels;

(c) an **AGPW engine** adjusting collaboration permissions;

(d) a **PoT validator** confirming safe combined operations;

(e) a **Trust Block register** documenting capacity-balancing lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 327. A system comprising, in any operable combination, one or more of:
(a) a **multi-agent plan refinement engine** optimizing coordinated tasks;
(b) a **Trust Criteria evaluator** ensuring refinements remain compliant;
(c) an **AGPW policy filter** controlling optimization boundaries;
(d) a **PoT verification gate** authorizing refinements;
(e) a **Trust Block ledger** encoding refinement lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 328. A system comprising, in any operable combination, one or more of:
(a) a **decomposition engine** splitting multi-agent tasks into domain-compliant subtasks;
(b) a **Trust Criteria evaluator** verifying each subtask's legitimacy;
(c) an **AGPW-constrained assignment module** distributing subtasks;
(d) a **PoT-based execution validator**;
(e) a **Trust Block** documenting task decomposition lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 329. A system comprising, in any operable combination, one or more of:
(a) a **temporal-coordination engine** synchronizing agent actions;
(b) a **Trust Criteria evaluator** confirming time-dependent constraints;
(c) an **AGPW governance layer** influencing permissible timing windows;
(d) a **PoT timing validator** authorizing synchronized execution;
(e) a **Trust Block trace** documenting coordinated timing lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 330. A system comprising, in any operable combination, one or more of:
(a) a **privacy-preserving observation-sharing engine** allowing agents to share vetted observations;
(b) a **Trust Criteria filter** evaluating permissible sharing;
(c) an **AGPW filter** ensuring domain-safe use;
(d) a **PoT-based approval module**;
(e) a **Trust Block ledger** recording observation-sharing events.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 331. A system comprising, in any operable combination, one or more of:

(a) an **agent-substitution module** replacing one agent in a multi-agent plan with another QPC-governed agent;

(b) a **Trust Criteria evaluator** verifying substitution validity;

(c) an **AGPW filter** determining permissible substitution boundaries;

(d) a **PoT execution gate** authorizing substitute participation;

(e) a **Trust Block** documenting substitution lineage.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 332. A system comprising, in any operable combination, one or more of:

(a) a **multi-agent fallback engine** identifying alternative plan paths;

(b) a **Trust Criteria evaluator** confirming fallback compliance;

(c) an **AGPW policy interpreter** adjusting fallback parameters;

(d) a **PoT validator** authorizing fallback plan execution;

(e) a **Trust Block** encoding fallback lineage.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 333. A system comprising, in any operable combination, one or more of:

(a) a **cross-agent safety envelope** defining allowable aggregate agent behavior;

(b) a **Trust Criteria evaluator** checking envelope compliance;

(c) an **AGPW engine** computing permissible envelope adjustments;

(d) a **PoT-based execution gate**;

(e) a **Trust Block** documenting safety-envelope lineage.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Family 9.3 — Federated Domain Governance

Defines a governance architecture for distributed AI ecosystems—where agents, enterprises, regulators, and jurisdictions each contribute policy signals. Rather than imposing a centralized authority, QPN enables a federated model: policies from multiple Human-Managed Trust Authorities are harmonized through AGPW, and their resulting governance parameters are applied consistently across AI agents in different sectors or geographies.

Ensures that AI agents operate lawfully and ethically across diverse regulatory regimes while maintaining a consistent global governance baseline. Agents dynamically adjust capability ceilings, routing decisions, content outputs, and delegation privileges based on federated policy signals. This ensures that regulatory updates, jurisdictional changes, or detected risks propagate instantly to all affected agents via PoT-based lineage.

Claim 334. A system comprising, in any operable combination, one or more of:

(a) a **federated governance layer** coordinating domain-specific policies across multiple Privacy Domains;

(b) a **Trust Criteria harmonization engine** mapping heterogeneous domain rules into unified constraints;

(c) an **AGPW evaluator** determining cross-domain policy weightings;

(d) a **PoT-based authorization module** validating each governance decision;

(e) a **Trust Block ledger** documenting inter-domain governance lineage.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 335. A system comprising, in any operable combination, one or more of:

(a) a **federated decision engine** aggregating governance inputs from multiple QPC-governed agents;

(b) a **Trust Criteria evaluator** validating each governance input;

(c) an **AGPW weighting mechanism** adjusting aggregated outcomes;

(d) a **PoT verifier** authorizing final governance decisions;

(e) a **Trust Block registry** encoding federated governance lineage.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 336. A system comprising, in any operable combination, one or more of:

(a) a **cross-domain policy translator** enabling interoperability between governance frameworks;

(b) a **Trust Criteria resolver** identifying policy conflicts;

(c) an **AGPW-based conflict-weighting module**;

(d) a **PoT-cleared conflict resolution engine**;

(e) a **Trust Block** documenting cross-domain policy alignment.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 337. A system comprising, in any operable combination, one or more of:

(a) a **federated supervision engine** monitoring QPC-governed agents across multiple domains;

(b) a **Trust Criteria compliance checker**;
(c) an **AGPW-governed escalation policy**;
(d) a **PoT-based authorization gate** for supervisory actions;
(e) a **Trust Block ledger** documenting supervisory lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 338. A system comprising, in any operable combination, one or more of:
(a) a **federated domain routing engine** determining permissible paths for multi-agent workflows;
(b) a **Trust Criteria evaluator** validating each candidate domain route;
(c) an **AGPW optimizer** computing trust-weighted routing priorities;
(d) a **PoT-based domain authorization mechanism**;
(e) a **Trust Block** documenting routing lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 339. A system comprising, in any operable combination, one or more of:
(a) a **domain-governance orchestrator** coordinating workflows across federated domains;
(b) a **Trust Criteria interpreter** evaluating domain-specific rules;
(c) an **AGPW governance engine** adjusting allowable orchestration;
(d) a **PoT-confirmed execution gate**;
(e) a **Trust Block** documenting orchestration lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 340. A system comprising, in any operable combination, one or more of:
(a) a **federated identity-verification engine** validating QPC-governed agent identity across domains;
(b) a **Trust Criteria evaluator** verifying identity legitimacy;
(c) an **AGPW influence model** determining identity trust-weight;
(d) a **PoT-based identity confirmation engine**;
(e) a **Trust Block** documenting identity-verification lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 341. A system comprising, in any operable combination, one or more of:
(a) a **federated consent-governance engine** regulating agent access across domains;

(b) a **Trust Criteria evaluator** mapping consent lineage to domain rights;
(c) an **AGPW filter** adjusting cross-domain consent enforcement;
(d) a **PoT-cleared consent validator**;
(e) a **Trust Block** documenting consent-governance lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 342. A system comprising, in any operable combination, one or more of:
(a) a **federated capability-governance engine** determining allowable agent abilities across domains;
(b) a **QRS evaluator** computing capability ceilings;
(c) an **AGPW policy-weighting engine** adjusting ceilings;
(d) a **PoT validator** authorizing cross-domain capability activation;
(e) a **Trust Block** documenting capability-governance lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 343. A system comprising, in any operable combination, one or more of:
(a) a **federated compliance-analysis engine** evaluating domain-level obligations;
(b) a **Trust Criteria** interpreter mapping obligations to executable constraints;
(c) an **AGPW-based compliance-weighting model**;
(d) a **PoT-cleared compliance-enforcement** module;
(e) a **Trust Block** recording compliance lineage across domains.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 344. A system comprising, in any operable combination, one or more of:
(a) a **federated audit engine** verifying compliance of agents and workflows across domains;
(b) a **Trust Criteria** evaluator identifying audit requirements;
(c) an **AGPW-governed audit policy**;
(d) a **PoT-authorized audit execution module**;
(e) a **Trust Block** documenting audit lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 345. A system comprising, in any operable combination, one or more of:
(a) a **federated escalation engine** determining when cross-domain interventions are required;
(b) a **Trust Criteria evaluator** identifying escalation triggers;

(c) an **AGPW policy model** computing escalation severity;
(d) a **PoT-cleared escalation executor**;
(e) a **Trust Block** documenting escalation lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 346. A system comprising, in any operable combination, one or more of:

(a) a **federated dispute-resolution engine** for multi-domain agent workflows;
(b) a **Trust Criteria evaluator** identifying disputed obligations;
(c) an **AGPW-based resolution policy**;
(d) a **PoT-confirmed resolution executor**;
(e) a **Trust Block** memorializing dispute-resolution lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 347. A system comprising, in any operable combination, one or more of:

(a) a **federated rights-management engine** applying domain-specific rights to multi-agent workflows;
(b) a **Trust Criteria resolver** determining allowable rights under lineage;
(c) an **AGPW rights-policy evaluator**;
(d) a **PoT-based authorization engine**;
(e) a **Trust Block** capturing rights-management lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 348. A system comprising, in any operable combination, one or more of:

(a) a **federated risk-governance engine** evaluating aggregate risk across domains;
(b) a **Trust Criteria translator** mapping risk rules;
(c) an **AGPW-based risk-weighting model**;
(d) a **PoT-cleared risk-enforcement engine**;
(e) a **Trust Block** documenting the risk-governance decision.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 349. A system comprising, in any operable combination, one or more of:

(a) a **federated domain-participation engine** determining whether an agent may operate within a given domain;
(b) a **Trust Criteria evaluator** verifying domain-entry requirements;
(c) an **AGPW policy mapping** inter-domain access limits;

(d) a **PoT-based entry validator**;
(e) a **Trust Block** encoding domain-entry lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 350. A system comprising, in any operable combination, one or more of:
(a) a **federated domain-governance controller** orchestrating multi-agent, multi-domain workflows;
(b)a **Trust Criteria evaluator** enforcing cross-domain constraints;
(c) an **AGPW-weighted governance model** determining lawful workflow boundaries;
(d)a **PoT authorization layer** validating all governance operations;
(e)a **unified Trust Block** documenting federated governance lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

GROUP 10 — ECONOMIC ARCHITECTURE, INCENTIVES & VALUE MECHANICS (Claims 351–390)

Establishes the economic layer of the Quantum Privacy Exchange (QPX), defining how value is created, measured, allocated, and distributed across the ecosystem in a trust-verified, privacy-preserving manner. Unlike traditional digital markets—where value flows are opaque, intermediaries capture disproportionate returns, and participants have little visibility into the outcomes they create—QPX enables every contribution, interaction, and resource flow to be linked to verifiable lineage & governed through cryptographic trust primitives.

Defines a universal **Contribution Value model** that determines how individuals, organizations, and AI agents generate economic value through their verified actions. This model is grounded in Trust Blocks, PoT attestations, QRS trust metrics, contractual constraints, and AGPW policy weightings. Instead of relying on subjective attribution, QPX assigns value objectively based on measurable contributions, improved outcomes, safety signals, or verified workflow efficiencies.

Group 10 also governs the **routing of incentives**, including Public-Benefit Derivative Rights (PBDRs), which allocate a portion of generated value toward human and societal benefit. Incentives may be distributed to participants, AI agents, enterprises, or public-benefit causes, all without exposing identity or sensitive data. The incentive mechanisms operate inside QPCs, ensuring rewards are aligned with lawful governance, participant rights & dynamic trust signals.

Finally, Group 10 defines the **settlement and economic infrastructure** that moves value through Exchange Networks and Liquidity Pools in a verifiable, auditable, and privacy-preserving manner. Every settlement event is trust-verified, every economic flow is governed by lineage metadata, and every allocation reflects policy, rights, and contributions. This transforms QPX into a self-funding ecosystem capable of supporting large-scale economic interactions across regulated sectors. This enables decentralized value creation and allocation without compromising privacy, legality, or fairness.

Family 10.1 — Contribution Value & Attribution

Introduces the mechanisms by which QPX measures, attributes, and evaluates economic contribution across participants, organizations, and AI agents. In traditional systems, attribution is subjective, fragmented, or distorted by intermediaries. QPX replaces these unreliable models with a **trust-verified attribution engine** grounded in PoT attestations, QRS trust scores, contractual context, lineage metadata, and outcome-based signals.

This engine evaluates how each participant's action—completing a workflow, sharing an EasyAccess link, providing expertise, or improving a societal metric—contributes to downstream value. Every contribution is cryptographically recorded, ensuring that value attribution is both objective and privacy-preserving. This provides for multi-party causality, delegation, and interdependency, preventing free-riding and enabling fair compensation.

This introduces foundational capabilities for value attribution across complex digital ecosystems. Enterprises in healthcare, finance, AI collaboration, content platforms, logistics, and public services all need reliable, privacy-preserving attribution mechanisms. By governing how contribution is measured and rewarded, these claims define the economic logic for next-generation incentive systems.

Claim 351. A system comprising, in any operable combination, one or more of:

- **(a)** a **Contribution Value engine** that derives trust-verified quantitative attribution from Resource Tokens, Solution Tokens, or Exchange Tokens;
- **(b)** a **lineage evaluator** that computes contribution weights using Trust Blocks;
- **(c)** a **Trust Criteria interpreter** that determines allowable attribution paths;
- **(d)** a **Proof-of-Trust (PoT) validator** confirming that contribution events satisfy domain, provenance, and contractual constraints;
- **(e)** a **distribution module** that allocates Contribution Value to participants according to verified lineage.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 352. A system comprising, in any operable combination, one or more of:

- **(a)** a **Contribution Value recorder** binding attribution to cryptographically sealed Trust Blocks;

(b) a **provenance engine** generating lineage graphs for each contributing participant;
(c) a **Trust Criteria filter** determining permissible attribution types;
(d) a **PoT verification layer** authorizing the inclusion of attribution records;
(e) an **allocation engine** distributing value in proportion to verified contributions.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 353. A system comprising, in any operable combination, one or more of:
(a) a **contribution-tracking module** capturing multi-party resource, workflow, or solution contributions;
(b) a **lineage-evaluation engine** computing weighted attribution from Trust Blocks;
(c) a **QRS-governed scaling mechanism** adjusting contribution weights;
(d) a **PoT-certified approval stage** validating computed weights;
(e) a **distribution record** encoded as a Trust Block.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 354. A system comprising, in any operable combination, one or more of:
(a) a **Contribution Value allocator** distributing trust-verified value among upstream contributors;
(b) a **Trust Criteria resolver** identifying permitted allocation paths;
(c) an **AGPW-weighted scoring mechanism** modifying attribution results;
(d) a **PoT verification module** approving final allocation sets;
(e) a **settlement Trust Block** documenting allocation lineage.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 355. A system comprising, in any operable combination, one or more of:
(a) a **multi-stage attribution engine** computing Contribution Value across sequential workflow steps;
(b) a **Trust Block lineage correlator** linking step-level contributions;
(c) a **Trust Criteria evaluator** determining which contributors qualify for attribution;
(d) a **PoT evaluation** enforcing compliance across all stages;
(e) a **final attribution record** encoded as a Trust Block.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 356. A system comprising, in any operable combination, one or more of:

(a) a **dynamic attribution engine** adjusting Contribution Value based on updated Trust Blocks;

(b) a **Trust Criteria propagation module** ensuring lineage continuity;

(c) a **QRS and AGPW weighting layer** recalculating attribution ceilings and priorities;

(d) a **PoT-secured approval process**;

(e) a **lineage-corrected attribution entry** encoded in Trust Blocks.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 357. A system comprising, in any operable combination, one or more of:

(a) a **multi-party attribution model** computing trust-governed contribution sets;

(b) a **provenance-evaluator** confirming that Resource Tokens used in solution formation satisfy lineage constraints;

(c) an **attribution policy engine** applying Trust Criteria;

(d) a **PoT verifier** authorizing attribution flows;

(e) an **encoded Trust Block** documenting multi-party attribution.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 358. A system comprising, in any operable combination, one or more of:

(a) an attribution-merging engine combining contributions from participants operating across different Privacy Domains;

(b) a Trust Criteria harmonizer enforcing cross-domain attribution rules;

(c) an AGPW-weighted adjustment engine;

(d) a PoT verification module validating merged attribution sets;

(e) a unified attribution Trust Block.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 359. A system comprising, in any operable combination, one or more of:

(a) a **contribution-index generator** assigning normalized Contribution Value scores across participants;

(b) a **Trust Criteria evaluator** determining index eligibility;

(c) a **QRS-based normalization engine**;

(d) a **PoT validator** approving index assignment;

(e) a **Trust Block documenting** the contribution-index lineage.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 360. A system comprising, in any operable combination, one or more of:

(a) a **contribution-splitting engine** dividing Contribution Value among derivative Resource Tokens;

(b) a **lineage evaluator** determining split proportions based on Trust Blocks;

(c) an **AGPW-adjusted scaling module**;

(d) a **PoT verifier** confirming split compliance;

(e) a **derivative-attribution Trust Block**.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 361. A system comprising, in any operable combination, one or more of:

(a) a **downstream-attribution engine** computing Contribution Value from sequential contributions;

(b) a **Trust Block aggregator** collecting lineage evidence from prior steps;

(c) a **Trust Criteria interpreter** determining allowable downstream flows;

(d) a **PoT-confirmation module** validating final attribution;

(e) a **downstream-attribution Trust Block**.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 362. A system comprising, in any operable combination, one or more of:

(a) a **Contribution Value governor** preventing attribution paths that violate domain, contractual, or lineage constraints;

(b) a **Trust Criteria resolver** identifying prohibited attribution;

(c) an **AGPW-governed enforcement module**;

(d) a **PoT-based denial engine**;

(e) a **Trust Block documenting the denial decision**.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Family 10.2 — Incentive Routing, PBDRs & Value Sharing

Defines the mechanisms through which value flows across the QPX ecosystem, including **incentive routing**, **trust-verified distributions**, and **Public-Benefit Derivative Rights (PBDRs)**. Incentives are not arbitrary; they are dynamically matched to contributions, trust signals, governance priorities, and public-benefit objectives.

Inside each QPC, incentive eligibility is evaluated using Trust Criteria, QRS scores, PoT lineage, and AGPW policy rules. Incentive flows adjust automatically as conditions evolve: if a participant becomes more trustworthy, creates more value, increases safety, or contributes to ecosystem health, their allocation increases. If trust erodes, allocation decreases. PBDRs ensure that a percentage of value generated by the ecosystem flows into public-benefit causes—such as healthcare outcomes, education, sustainability, or ecological restoration—without exposing personal or proprietary data.

This governs how incentives and value-sharing mechanisms operate across the entire digital economy. Platforms that rely on contribution-based rewards, referral loops, loyalty systems, public-benefit offsets, or AI-driven engagement will require these claims. PBDRs introduce a groundbreaking mechanism for linking economic success to social good.

Claim 363. A system comprising, in any operable combination, one or more of:

(a) an **incentive-routing engine** distributing value among contributors based on Contribution Value;
(b) a **Trust Criteria evaluator** determining permissible incentive flows;
(c) a **PBDR routing module** redirecting prohibited or restricted value to Public-Benefit Derivative Rights;
(d) a **PoT verification layer** authorizing routed flows;
(e) a **Trust Block capturing incentive-routing lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 364. A system comprising, in any operable combination, one or more of:

(a) a **value-sharing engine** distributing trust-verified value to eligible participants;
(b) a **Trust Criteria interpreter** enforcing contractual or ethical constraints;
(c) a **PBDR evaluator** determining which value flows require redirection;
(d) a **PoT validator** confirming routing legitimacy;
(e) a **Trust Block documenting distribution lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 365. A system comprising, in any operable combination, one or more of:

(a) an **AGPW-adjusted incentive engine** modifying value-sharing outcomes based on policy weights;
(b) a **Trust Criteria evaluator** determining allowable incentive modifications;
(c) a **PBDR routing mechanism** for non-permissible flows;
(d) a **PoT confirmation layer**;
(e) a **Trust Block encoding AGPW-adjusted incentive lineage**.

Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 366. A system comprising, in any operable combination, one or more of:

(a) a **multi-party incentive computation engine** aggregating trust-verified entitlements;
(b) a **Trust Criteria filter** determining allocation eligibility;
(c) a **PBDR-directed override routing mechanism**;
(d) a **PoT authorization step**;
(e) a **collective incentive Trust Block recording distribution lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 367. A system comprising, in any operable combination, one or more of:

(a) a **value-routing engine** mapping economic flows to contributors according to lineage;
(b) a **Trust Criteria interpreter** applying domain-specific routing constraints;
(c) a **PBDR enforcement layer** routing restricted value to public-benefit recipients;
(d) a **PoT validation step**;
(e) a **Trust Block documenting the routed value flow**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 368. A system comprising, in any operable combination, one or more of:

(a) an **incentive-balancing engine preventing** over-compensation relative to verified Contribution Value;
(b) a **Trust Criteria evaluator** identifying impermissible incentive imbalances;
(c) a **PBDR routing mechanism** for excess value;
(d) a **PoT-based enforcement engine**;
(e) a **Trust Block documenting balancing lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 369. A system comprising, in any operable combination, one or more of:

(a) an **incentive-prioritization engine** ranking contributors using Trust Criteria;
(b) an **AGPW influence model** adjusting priority scores;
(c) a **PBDR routing mechanism** for ineligible priority recipients;
(d) a **PoT validator approving** prioritized incentive paths;

(e) a **Trust Block documenting prioritization lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 370. A system comprising, in any operable combination, one or more of:

(a) a **cross-domain incentive-routing engine** distributing value across different Privacy Domains;
(b) a **Trust Criteria harmonizer** evaluating eligibility across domain boundaries;
(c) a **PBDR routing layer** for incompatible flows;
(d) a **PoT validation step**;
(e) a **Trust Block documenting cross-domain routing lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 371. A system comprising, in any operable combination, one or more of:

(a) an **incentive-aggregation engine** consolidating multiple eligible incentive flows;
(b) a **Trust Criteria filter** determining allowable aggregation combinations;
(c) a **PBDR module** for removing ineligible amounts;
(d) a **PoT-based aggregation validator**;
(e) a **Trust Block documenting aggregated incentive lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 372. A system comprising, in any operable combination, one or more of:

(a) a **fractional incentive-routing module** dividing incentive flows among fine-grained contribution lineages;
(b) a **Trust Block analyzer** determining fractional proportions;
(c) a **PBDR redirection mechanism** for restricted fractions;
(d) a **PoT compliance validator**;
(e) a **Trust Block documenting fractional routing decisions**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 373. A system comprising, in any operable combination, one or more of:

(a) an **incentive-substitution engine** replacing ineligible recipients with compliant substitutes;
(b) a **Trust Criteria evaluator** identifying substitute eligibility;
(c) a **PBDR-assisted fallback mechanism**;

(d) a **PoT verification stage**;
(e) a **Trust Block recording incentive substitution lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 374. A system comprising, in any operable combination, one or more of:

(a) an **incentive-routing governor** applying Trust Criteria to enforce routing constraints;
(b) an **AGPW policy adjuster** influencing routing decisions;
(c) a **PBDR fallback module** for disallowed paths;
(d) a **PoT verification engine**;
(e) a **Trust Block documenting routing-governance lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 375. A system comprising, in any operable combination, one or more of:

(a) a **value-sharing forecaster** predicting allowable incentive flows;
(b) a **Trust Criteria engine** evaluating forecasted eligibility;
(c) a **PBDR routing module** adjusting forecast outputs;
(d) a **PoT confirmation step** validating forecasted-routing decisions;
(e) a **Trust Block documenting forecast lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Family 10.3 — Network Economics, Settlements & Exchange Fee Flows

Defines the infrastructure that enables **trust-verified settlement, multi-party value flows, liquidity management, and Exchange Fee distribution**. Every economic transaction in QPX is validated through PoT attestations and executed inside QPC-governed workflows. Identity, account numbers, and proprietary data are never exposed. Instead, settlement instructions propagate through Privacy Domains with complete lineage verification.

This also establishes the mechanisms that direct Exchange Fees and liquidity flows back to participants, accelerators, enterprises, ecosystem operators, and public-benefit causes. Because QPX operates across regulated sectors, settlement flows must remain fully compliant with contractual obligations, jurisdictional requirements, and governance policies. The system provides automated enforcement, programmable fee distribution, multi-hop routing, and fallback guarantees that maintain economic integrity across the network. These claims define the business model for operators of QPX Exchange Networks and form the basis for long-term licensing revenues across industries and governments.

Claim 376. A system comprising, in any operable combination, one or more of:

(a) an **Exchange Fee engine** computing trust-verified fee amounts for transactions executed through Exchange Networks;
(b) a **Trust Criteria evaluator** determining eligible fee recipients;
(c) an **AGPW-governed fee-adjustment module** applying policy-weighted parameters;
(d) a **PoT verification layer** authorizing computed fee flows;
(e) a **settlement Trust Block documenting fee lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) Quantum Privacy Cells (QPCs); (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 377. A system comprising, in any operable combination, one or more of:

(a) a **settlement engine** performing trust-verified matching and clearing of Resource Tokens, Solution Tokens, and Exchange Tokens;
(b) a **Trust Criteria resolver** enforcing provenance and contractual constraints;
(c) an **Exchange Fee apportionment module** mapping fee flows to eligible participants;
(d) a **PoT-based authorization module**;
(e) a **Trust Block capturing multi-party settlement lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 378. A system comprising, in any operable combination, one or more of:

(a) a **value-routing settlement engine** determining multi-party economic flows across Exchange Networks;
(b) a **Trust Criteria evaluator** identifying permitted routing paths;
(c) an **AGPW-weighted economic-layer adjuster**;
(d) a **PoT confirmation stage authorizing the settlement**;
(e) a **settlement Trust Block encoding routing lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 379. A system comprising, in any operable combination, one or more of:

(a) a **cross-network economic reconciliation engine** linking multiple Exchange Networks;
(b) a **Trust Criteria interpreter** harmonizing settlement requirements;
(c) an **AGPW influence model** adjusting reconciliation outcomes;
(d) a **PoT verification module**;

(e) a **Trust Block documenting reconciliation lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 380. A system comprising, in any operable combination, one or more of:

(a) a **multi-pool settlement engine** performing coordinated settlement across Resource Pools, Token Pools, and Liquidity Pools;
(b) a **Trust Criteria resolver** evaluating cross-pool constraints;
(c) an **AGPW-governed pool-selection module**;
(d) a **PoT-validated settlement executor**;
(e) a **Trust Block documenting coordinated pool-settlement lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 381. A system comprising, in any operable combination, one or more of:

(a) an **Exchange Fee routing engine** distributing fees among Accelerators, contributors, and other eligible entities;
(b) a **Trust Criteria evaluator** confirming routing eligibility;
(c) an **AGPW policy-modifier** shaping distribution priorities;
(d) a **PoT validator authorizing fee routing**;
(e) a **Trust Block documenting fee-routing lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 382. A system comprising, in any operable combination, one or more of:

(a) a **treasury-governance engine** determining permitted uses of trust-verified fee reserves;
(b) a **Trust Criteria interpreter** enforcing treasury rules;
(c) an **AGPW-based policy engine** shaping treasury allocation dynamics;
(d) a **PoT validator confirming** allowable disbursements;
(e) a **Trust Block documenting treasury-governance lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 383. A system comprising, in any operable combination, one or more of:

(a) a **settlement-balancing engine** ensuring multi-party settlement flows respect allowable lineage;
(b) a **Trust Criteria resolver** identifying constraint violations;
(c) an **AGPW governance layer** applying corrective weighting;

(d) a **PoT-based enforcement step**;
(e) a **Trust Block documenting settlement-balancing lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 384. A system comprising, in any operable combination, one or more of:

(a) an **economic fallback-routing engine** identifying substitutes when a settlement path fails;
(b) a **Trust Criteria evaluator** testing substitute compliance;
(c) an **AGPW-based fallback policy**;
(d) a **PoT verification module** authorizing fallback settlement;
(e) a **Trust Block encoding fallback-settlement lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 385. A system comprising, in any operable combination, one or more of:

(a) a **settlement-prioritization engine** ranking economic flows based on Contribution Value or policy weights;
(b) a **Trust Criteria interpreter** verifying ranking legitimacy;
(c) an **AGPW-based priority adjuster**;
(d) a **PoT confirmation step**;
(e) a **Trust Block documenting prioritized-settlement lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 386. A system comprising, in any operable combination, one or more of:

(a) a **cross-domain settlement engine** performing trust-governed clearing across multiple Privacy Domains;
(b) a **Trust Criteria harmonizer** enforcing inter-domain settlement rules;
(c) an **AGPW governance model** shaping inter-domain economic flows;
(d) a **PoT validator** authorizing cross-domain settlement;
(e) a **Trust Block capturing settlement lineage across domains**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) Proof-of-Trust (PoT); (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 387. A system comprising, in any operable combination, one or more of:

(a) a **macro-level network economics engine** modeling aggregate value flows through Exchange Networks;
(b) a **Trust Criteria evaluator** determining permissible aggregate behavior;

(c) an **AGPW influence engine** weighting network-wide economic policies;
(d) a **PoT verification layer** authorizing macro-economic adjustments;
(e) a **Trust Block encoding macro-economic lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 388. A system comprising, in any operable combination, one or more of:

(a) a **liquidity-governance engine** determining allowable liquidity flows across QPN-governed pools;
(b) a **Trust Criteria evaluator** testing liquidity constraints;
(c) an **AGPW-weighted liquidity-policy model**;
(d) a **PoT validator** enforcing liquidity governance;
(e) a **Trust Block documenting liquidity-governance lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 389. A system comprising, in any operable combination, one or more of:

(a) a **network-fee normalization engine** ensuring Exchange Fee rates remain compliant with domain and Trust Criteria constraints;
(b) an **AGPW-based adjustment engine**;
(c) a **PoT validation module** authorizing normalized fee outputs;
(d) a **Trust Block documenting fee-normalization lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.

Claim 390. A system comprising, in any operable combination, one or more of:

(a) an **integrated value-settlement controller** synchronizing Exchange Fees, multi-party settlements, and incentive routing;
(b) a **Trust Criteria evaluator** enforcing economic constraints;
(c) an **AGPW-weighted economic governance engine**;
(d) a **PoT authorization layer** validating integrated settlement outcomes;
(e) a **unified Trust Block representing complete economic-settlement lineage**.
Wherein the system operates within a QPN-enabled infrastructure comprising at least one of: (i) QPCs; (ii) Privacy Domains; (iii) Trust Criteria; (iv) PoT; (v) Trust Blocks; or (vi) EasyAccess workflow threads.