Q-Fabric (Formerly C2Q): An Enterprise Architecture for Sovereign Hybrid Quantum-Classical Computing, Verifiable Execution, and Post-Quantum Settlement

Author: Qantum One **Publication Date:** October 29, 2026 **Document Classification:** Enterprise Reference Architecture & Technical Whitepaper (v2.0) **Nomenclature Transition Notice:** *This specification supersedes the March 2025 "Classic-to-Quantum (C2Q)" proposal. To reflect the transition from one-way classical-to-quantum blockchain bridging to bidirectional, rack-scale hybrid orchestration and cryptographic execution auditing, the platform is formally renamed **Q-Fabric (Sovereign Hybrid Quantum-Classical Orchestration & Attestation Fabric)**, and its middleware interface is designated the **HQCA (Hybrid Quantum-Classical Attestation) Gateway API**.*

I. Executive Summary and Paradigm Shift

The convergence of data-center-deployable quantum processors, verifiable quantum computation, and standardized post-quantum cryptography (PQC) has fundamentally altered enterprise high-performance computing (HPC) and distributed ledger security. Historically, quantum computing remained confined to specialized laboratory environments requiring external dilution refrigerators, dedicated facilities, and bespoke physics teams, while enterprise blockchain networks relied on elliptic-curve and RSA cryptographic primitives vulnerable to Shor's and Grover's algorithms. Between March 2025 and October 2026, three watershed developments moved hybrid quantum-classical computing from theoretical exploration into production data center deployment:

1. **Sovereign In-Rack Silicon-Spin Quantum Acceleration:** Following the March 2025 debut of the Equal1 Bell-1 server and a $60 million funding round in January 2026 led by the Ireland Strategic Investment Fund (ISIF), Equal1 and Dell Technologies unveiled **RacQ** in May 2026. Powered by the **UnityQ** Quantum System-on-Chip (QSoC) fabricated on GlobalFoundries 22FDX commercial CMOS with on-die 300 mK CryoCMOS control and embedded ARM cores, RacQ integrates directly alongside a Dell PowerEdge R770 server within a standard 42U rack, drawing 1,600 W from a single-phase socket and executing 10,000 to 100,000 variational shots per second at sub-millisecond rack latency.
2. **Coherent Quantum Annealing and Verifiable Witness Protocols:** In May 2025, D-Wave Quantum Inc. achieved general availability of its **Advantage2** superconducting quantum annealing system featuring the 4,400+ qubit Zephyr-12 (Z12) processor with 20-way connectivity and over 40,000 couplers. Concurrently, in February 2026, D-Wave published Revision 3 of its verifiable quantum hash framework (arXiv:2503.14462v3), demonstrating cross-QPU probabilistic witness validation with an uncertainty metric of \sigma_W = 0.16 across distributed quantum processors.

3. **Federal Post-Quantum Mandates and Native Layer-1 Account Abstraction:** Building on its August 2024 standardization of FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA), the National Institute of Standards and Technology (NIST) selected HQC (Hamming Quasi-Cyclic, designated for FIPS 207) in March 2025 as its code-based backup key encapsulation mechanism, while the White House Office of Management and Budget (OMB) issued Memorandum M-26-15 in June 2026 mandating accelerated federal PQC migration ahead of the 2035 National Security System deadline. Simultaneously, the Ethereum Foundation established a dedicated Post-Quantum Security team in January 2026 and published a formal roadmap in February 2026 introducing native post-quantum Frame Transactions (EIP-8141) and secondary signature support (EIP-7932) targeted for the 2027 Hegotá hard fork.

The Strategic Pivot from C2Q to Q-Fabric: Earlier architectural proposals attempted to use 6-qubit gate-based silicon processors to mine blocks on a D-Wave Proof of Quantum Work (PoQW) blockchain and incentivize decentralized public AI training via native tokens. Rigorous physical auditing demonstrates that a 6-qubit Hilbert space (2^6 = 64 complex amplitudes) can be simulated trivially on classical processors in microseconds, violating PoQW spoof resistance, while unencrypted classical-to-quantum bridges expose legacy ECDSA public keys prior to quantum ingress.

Q-Fabric resolves these physical and cryptographic contradictions by replacing cross-hardware cryptocurrency mining with a four-tier **Sovereign Hybrid Quantum-Classical Compute (HQCC) Orchestration and Cryptographic Attestation Platform**. Rather than forcing gate-based processors to emulate quantum annealers, Q-Fabric leverages Dell's Quantum Intelligent Orchestrator to route sub-millisecond variational subroutines to co-located on-premise Equal1 RacQ nodes while dispatching large-scale combinatorial optimization models (up to 4,400+ physical qubits or 2 million hybrid variables) to D-Wave Advantage2 solvers. D-Wave's hyperplane witness mathematics (arXiv:2503.14462v3) is repurposed into a **Proof of Quantum Execution (PoQE)** audit mechanism, anchored to Ethereum-compatible settlement layers via STARK-batched EIP-8141 Frame Transactions secured end-to-end by NIST FIPS 203 and FIPS 204 cryptography.

II. Foundational Technologies and October 2026 Baseline

A. Equal1 RacQ and the UnityQ CMOS Quantum System-on-Chip (QSoC)

The Equal1 **RacQ** server, unveiled globally on May 14, 2026, represents the production evolution of the March 2025 Bell-1 prototype and the world's first deployable rack-mounted silicon-spin quantum computer designed for standard 19-inch (42U) enterprise data center frames. Backed by over $85 million in total venture and sovereign capital—including a $60 million (€51.5 million) round in January 2026 led by ISIF with participation from Atlantic Bridge, the European Innovation Council (EIC) Fund, Matterwave Ventures, and Enterprise Ireland—Equal1 has transitioned silicon-spin quantum computing into high-volume commercial CMOS foundry manufacturing alongside partners such as GlobalFoundries and TSMC. In July 2026, the European Space Agency (ESA) contracted Equal1 to install an on-premises quantum system at the European Space Research Institute (ESRIN) to accelerate Earth Observation

disaster response and environmental data processing.

At the core of RacQ is the **UnityQ** processor, fabricated on the commercial GlobalFoundries 22FDX CMOS process featuring 35 monolithic quantum cells and 6 active linear silicon-spin qubits. Unlike conventional quantum architectures where control electronics reside outside the cryostat—introducing interconnect latency, thermal load, and signal attenuation—UnityQ pioneers **CryoCMOS** integration. Analog radio-frequency (RF) generation, parity readout circuitry, cycle-accurate digital timing logic, and embedded ARM processor cores operate at 300 mK (0.3 Kelvin) directly adjacent to the silicon quantum dots on the same die. This architecture collapses physical distance to microns, enabling an on-die machine learning detect-decode-correct loop at sub-cycle latency. Furthermore, through Equal1's April 2026 partnership with Q-CTRL, RacQ embeds autonomous calibration and error-mitigation software directly into the platform, maintaining peak gate fidelities without human physicist intervention.

Thermally and mechanically, RacQ eliminates external liquid helium infrastructure via a self-contained, closed-cycle air-cooled sorption cryocooler delivering 200 mW of cooling power at 4.2 K and 160\ \mu\text{W} at 0.38 K (requiring 117 CFM airflow, a 38-hour total cooldown from 300 K to 0.3 K, and a 5,000-hour continuous service interval). The standalone RacQ enclosure measures 600 \times 1200 \times 2000\text{ mm} and weighs 200 kg, while the full hybrid rack configuration co-located with a Dell PowerEdge R770 server and Dell PowerSwitch networking weighs 400 kg and plugs into a standard 208/240V, 16A single-phase electrical socket consuming 1,600 W.

In typical operating conditions on UnityQ silicon, RacQ achieves an average single-qubit (1Q) gate fidelity of 99.9% at a 140 ns duration (randomized Clifford benchmarking), an average two-qubit (2Q) gate fidelity of 99.3% at a 200 ns duration (interleaved randomized benchmarking), and a parity readout fidelity of 99% to 99.9% at a 10\ \mu\text{s} readout duration. These fast silicon gate times allow RacQ to execute 10,000 to 100,000 variational shots per second. However, system architects must account for the **linear array SWAP routing constraint**: because the 6 spin qubits are arranged in a 1D chain with nearest-neighbor coupling, entangling Qubit 1 and Qubit 6 requires 4 SWAP gates (equivalent to 12 additional CNOT gates). This routing tax reduces effective end-to-end 2Q fidelity across the array to:

$$F_{\text{effective}} = (0.993)^{13} \approx 91.2\%$$

while expanding total gate execution duration from 200 ns to 2.6\ \mu\text{s}. Consequently, Q-Fabric transpilers restrict RacQ compilation to shallow, nearest-neighbor variational ansätze.

Hardware Specification	Legacy Bell-1 Baseline (March 2025)	Production RacQ Baseline (October 2026)	Q-Fabric Architectural Role
System Architecture	Standalone Bell-1 rack node (600 \times 1000 \times 1600\text{ mm}, 200 kg)	Equal1 RacQ (600 \times 1200 \times 2000\text{ mm}, 200 kg standalone / 400 kg in Dell 42U HQCC rack)	Co-located in-rack peer accelerator alongside Dell PowerEdge R770.
Quantum Processor (QPU)	UnityQ 6-qubit silicon processor (QSoC planned for future)	UnityQ QSoC on GlobalFoundries 22FDX CMOS (35 monolithic cells, 6 active linear spin qubits)	Executes compact variational loops (10k–100k shots/sec) inside sovereign perimeter.
Cryogenic Control &	Rack-mounted external	On-die 300 mK	Sub-millisecond hybrid

Hardware Specification	Legacy Bell-1 Baseline (March 2025)	Production RacQ Baseline (October 2026)	Q-Fabric Architectural Role
Autonomy	control electronics	CryoCMOS RF/digital logic + embedded ARM cores + Q-CTRL autocalibration	loops; zero-touch calibration over 5,000-hour intervals.
Gate & Readout Metrics	1Q: 99.40%; 2Q (CZ): 98.40%; Readout: >99.9%	1Q: 99.9% (140 ns); 2Q: 99.3% nearest-neighbor (200 ns) / 91.2% end-to-end; Readout: 99%–99.9% (10\ \mu\text{s})	High-speed sampling for shallow nearest-neighbor circuits.
Cryogenics & Electrical	0.3 K closed-cycle cooler; 1,600 W standard socket	Air-cooled sorption cooler (160\ \mu\text{W} @ 0.38 K, 38h cooldown); 1,600 W @ 208/240V 16A single-phase	Operates in standard -15^\circ\text{C} to +45^\circ\text{C} data centers without liquid helium.

B. D-Wave Advantage2 and Proof of Quantum Execution (PoQE)

For large-scale combinatorial optimization and verifiable quantum state attestation that exceed the 64-amplitude Hilbert space of a 6-qubit gate processor, Q-Fabric integrates D-Wave's **Advantage2** annealing architecture. Released for general availability on May 20, 2025, Advantage2 features the Zephyr-12 (Z12) superconducting QPU containing over 4,400 qubits and more than 40,000 couplers operating at 15.4 mK to 20 mK. Compared to the 15-way connectivity of the previous-generation Pegasus topology, Zephyr provides 20-way qubit connectivity, a 40% increase in energy scale, 2\times longer coherence time, and 4\times lower noise. When benchmarked on 1,650-node (12 \times 12 \times 12) 3D spin-glass lattices with tunable quadratic weight precision (r = 16, 128), Advantage2 operating in the fast coherent annealing regime surpasses legacy Advantage systems by over 10,000\times in time-to-solution. Furthermore, D-Wave's Leap cloud service integrates Advantage2 with nonlinear hybrid solvers capable of processing up to 2 million variables and constraints, supplemented in June 2026 by D-Wave's error-aware gate-model simulator and in October 2026 by expanding European on-premises Advantage2 deployments.

Critically, Q-Fabric adapts the mathematical formalism of Amin et al.'s February 9, 2026 publication, *Blockchain with proof of quantum work* (arXiv:2503.14462v3), and its accompanying open-source solver suite (dwave-examples/quantum-blockchain) from standalone cryptocurrency block mining into a verifiable **Proof of Quantum Execution (PoQE)** protocol. In Q-Fabric, when an enterprise client dispatches a high-value optimization or spin-glass simulation workload \mathcal{M} to an Advantage2 QPU, the execution node generates a cryptographic witness proof across four formal stages:

1. **Deterministic Preprocessing:** The workload specification and execution nonce \mathcal{M} are transformed deterministically into a set of coupler weights \Theta = \text{Random}(\mathcal{M}) with zero local magnetic biases (h_i = 0 and J_{ij} = \Theta(\mathcal{M})). In accordance with the 2026 D-Wave reference specification, dependence on the volatile wall-clock timestamp is excluded from the hash input so that

independent auditors can deterministically reconstruct the exact problem Hamiltonian.

2. **Coherent Unitary Evolution:** The parameter set \Theta governs the continuous-time unitary evolution U_\Theta of an N_Q-qubit quantum system from initial state \vert{}\psi_0\rangle to final state \vert{}\psi_\mathcal{M}\rangle = U_\Theta\vert{}\psi_0\rangle, characterized by the pure state density matrix \rho_\mathcal{M} = \vert{}\psi_\mathcal{M}\rangle\[span_130](start_span)[span_130](end_span)langle\psi_\mathcal{M}\vert{}. Because commercial Advantage2 processors exhibit higher energy scales than the Advantage2_prototype2 baseline schedule and cannot reduce annealing time below the 5-nanosecond hardware floor, Q-Fabric normalizes cross-QPU unitary dynamics by scaling down the problem Hamiltonian energy coefficients.
3. **Observable Postprocessing:** Using N_{\text{reads}} = 600 quantum annealing samples (optimized in the 2026 protocol to reduce QPU access overhead below 1 second), the system computes a vector of expected multi-qubit observables (witnesses) W(\rho_\mathcal{M}) derived from single- and multi-qubit spin correlations \langle\sigma_i^z\rangle, \langle\sigma_i^z\sigma_j^z\rangle, \langle\sigma_i^z\sigma_j^z\sigma_k^z\rangle.
4. **Hyperplane Digitalization and Probabilistic Validation:** Each continuous witness element W_\alpha is discretized into a binary bit via the Heaviside step function \theta(x) relative to a threshold hyperplane W_{0\alpha}:

$$\mathcal{H}_\alpha = \theta(W_\alpha - W_{0\alpha}) = \begin{cases} 0, & W_\alpha < W_{0\alpha} \\ 1, & W_\alpha \ge W_{0\alpha} \end{cases}$$

yielding a 64-bit quantum execution hash $\mathcal{H}(\mathcal{M}) = \mathcal{H}_1\mathcal{H}_2\dots\mathcal{H}_{64}$. Because quantum sampling is intrinsically probabilistic, an auditing QPU validating $\mathcal{H}(\mathcal{M})$ may observe bit flips when W_α lies close to the hyperplane boundary $W_{0\alpha}$. Rather than rejecting the proof on a single bit mismatch, Q-Fabric computes a confidence score where any discrepant bit reduces validator confidence by a factor of $(1 - P_\alpha)/P_\alpha$, accepting the Proof of Quantum Execution when cross-QPU witness uncertainty remains within the calibrated 2026 Advantage2 tolerance of $\sigma_W \le 0.16$.

C. Post-Quantum Cryptography (PQC) and Federal Compliance Architecture

To protect enterprise workloads, API payloads, and ledger settlement against cryptanalytically relevant quantum computers (CRQCs) running Shor's algorithm against RSA/ECC and Grover's quadratic speedup against symmetric primitives, Q-Fabric enforces a strict, NIST-compliant PQC security baseline. All deprecated or broken candidate schemes cited in earlier literature—specifically isogeny-based SIKE and multivariate Rainbow (both broken classically), NTRU (superseded by ML-KEM), Classic McEliece (declined for NIST standardization due to ~1 MB public keys), and BIKE (retained only as a non-standardized research candidate)—are permanently excluded from the Q-Fabric cryptographic suite.

Q-Fabric's cryptographic layer is governed by the finalized NIST FIPS standards and 2025–2026 federal directives, including White House OMB Memorandum M-26-15 (*Execution of the Migration to Post-Quantum Cryptography*, June 24, 2026), the June 2026 Executive Order accelerating Cryptographic Module Validation Program (CMVP) certifications, and National Security Agency (NSA) National Security System (NSS) mandates requiring PQC across

network equipment in 2026 ahead of complete federal migration by 2035:

- **Transit Key Establishment (FIPS 203 / ML-KEM & FIPS 207 / HQC):** All HQCA gateway channels mandate **FIPS 203 (ML-KEM)**, the module-lattice key encapsulation mechanism standardized in August 2024. To guarantee mathematical diversity against potential future lattice cryptanalysis, Q-Fabric incorporates crypto-agility for **HQC (Hamming Quasi-Cyclic)**, selected by NIST on March 11, 2025 (NIST IR 8545) at the conclusion of Round 4 to become **FIPS 207**. Unlike probabilistic code-based decoders that suffer from decoding failure rate (DFR) vulnerabilities, HQC employs a deterministic code-based construction that always decrypts correctly, offering constant-time implementation safety, ~7 KB public keys, and ~14 KB ciphertexts. While NIST had not yet published the public draft of FIPS 207 as of October 2026, Q-Fabric schedules production dual-KEM (ML-KEM + HQC) deployment for 2027 upon final FIPS 207 ratification.
- **Digital Signatures (FIPS 204 / ML-DSA & FIPS 205 / SLH-DSA):** Q-Fabric designates **FIPS 204 (ML-DSA)** as the mandatory default digital signature algorithm for workload authentication, rack telemetry signing, and API attestation. Protocol buffers and network frames are explicitly sized to accommodate standardized FIPS 204 signature footprints: **2,420 bytes** for ML-DSA-44 (Security Category 2), **3,309 bytes** for ML-DSA-65 (Security Category 3, Q-Fabric default), and **4,627 bytes** for ML[span_153](start_span)[span_153](end_span)-DSA-87 (Security Category 5). For long-term root state anchoring requiring non-lattice mathematical assumptions, Q-Fabric supports **FIPS 205 (SLH-DSA / SPHINCS+)** stateless hash-based signatures as a high-assurance backup.
- **Deferral of FIPS 206 (FN-DSA / FALCON) for Leaf Signing:** Although NIST submitted the draft standard for **FIPS 206 (FN-DSA)**—an NTRU-lattice signature scheme using Fast-Fourier Transform (FFT) and LDL trees to achieve compact signature sizes—for internal approval on August 28, 2025, no Initial Public Draft (IPD) or Federal Register notice had been released as of October 2026. Furthermore, as documented by NIST cryptographers, FN-DSA signing requires strict native or emulated IEEE-754 binary64 floating-point arithmetic without fused multiply-add instructions, forbids deterministic signing and seed export, and is vulnerable to timing side-channel key leakage if Gaussian discrete sampling deviates from Known Answer Tests (KATs). Consequently, Q-Fabric restricts future FN-DSA adoption to root/intermediate CA certificates issued in controlled hardware security modules (HSMs), relying exclusively on integer-lattice ML-DSA for high-frequency leaf transactions.

| Standard Designation | Algorithm Name | Mathematical Foundation | October 2026 Status | Key / Signature Footprint | Q-Fabric Deployment Policy | | :--- | :--- | :--- | :--- | :--- | :--- | | **FIPS 203** | **ML-KEM** (CRYSTALS-Kyber) | Module-Lattice KEM | **Finalized Standard** (Aug 2024) | Compact lattice keys/ciphertexts | Primary mandatory KEM for all HQCA mTLS 1.3 channels. | | **FIPS 204** | **ML-DSA** (CRYSTALS-Dilithium) | Module-Lattice Signature | **Finalized Standard** (Aug 2024) | Signatures: 2,420 B (-44), 3,309 B (-65), 4,627 B (-87) | Primary mandatory signature scheme (ML-DSA-65 default). | | **FIPS 205** | **SLH-DSA** (SPHINCS+) | Stateless Hash-Based Signature | **Finalized Standard** (Aug 2024) | Signatures: Tens of kilobytes | Non-lattice fallback for root anchors and hybrid ERC-4337 wallets. | | **FIPS 206** | **FN-DSA** (FALCON) | NTRU-Lattice / FFT Gaussian Sampling | **In Development** (Submitted Aug 2025; no public draft as of Oct 2026) | Compact signatures (~666–1,280 B) | Deferred for leaf nodes due to IEEE-754 floating-point signing complexity. | | **FIPS 207** | **HQC** (Hamming Quasi-Cyclic) | Code-Based Deterministic KEM | **Selected Mar 2025** (NIST IR 8545; no draft as of Oct 2026; final 2027) | Public Key: ~7 KB; Ciphertext: ~14 KB | Scheduled for 2027 production rollout as

non-lattice backup KEM. |

III. The Q-Fabric Enterprise Architecture (Formerly C2Q)

A. System Architecture Overview and Four-Tier Component Interaction

Q-Fabric replaces the legacy two-layer blockchain-bridge model with a modular, four-tier enterprise stack that unifies on-premise silicon-spin quantum computing, cloud superconducting quantum annealing, post-quantum middleware attestation, and native post-quantum blockchain settlement:

1. **Tier 1: Enterprise Client & Post-Quantum Origin Layer:** Enterprise applications, quantitative risk engines, defense logistics platforms, and smart contract accounts originate hybrid compute jobs and settlement transactions. Crucially, all payloads are signed at the point of origin using FIPS 204 ML-DSA-65 or Ethereum EIP-8141 Frame Transaction commitments, ensuring that no vulnerable classical ECDSA public keys are ever broadcast over network links.
2. **Tier 2: The HQCA (Hybrid Quantum-Classical Attestation) Gateway & Dell Orchestrator:** Acting as the secure control plane, the HQCA Gateway terminates FIPS 203 ML-KEM mutually authenticated gRPC streams, verifies ML-DSA client signatures via CMVP-validated cryptographic modules, and passes validated workload graphs to the **Dell Quantum Intelligent Orchestrator**. The orchestrator analyzes problem dimensionality, shot requirements, connectivity graphs, and data sovereignty policies to route subroutines across Tier 3 quantum resources.
3. **Tier 3: Heterogeneous Quantum Execution Layer (Sovereign Rack + Cloud Annealer):**
    - **On-Premise Sovereign HQCC Node (Equal1 RacQ + Dell PowerEdge R770):** Co-located inside the enterprise's own 42U rack connected via Dell PowerSwitch networking, the Dell PowerEdge R770 CPU/GPU server handles classical pre- and post-processing while offloading high-frequency variational subroutines (10,000–100,000 shots/sec) across a sub-millisecond local bus to the 6-qubit Equal1 RacQ UnityQ processor. Sensitive data never leaves the physical perimeter.
    - **Cloud Annealing Co-Processor (D-Wave Advantage2):** For non-air-gapped combinatorial optimization, spin-glass simulation, and constrained scheduling workloads requiring thousands of qubits or millions of variables, the orchestrator dispatches problems to D-Wave Advantage2 Zephyr-12 QPUs (4,400+ qubits) or Leap Stride/Nonlinear hybrid solvers.
4. **Tier 4: Verifiable Proof of Quantum Execution (PoQE) & Post-Quantum Settlement Layer:** Upon workload completion, Tier 3 nodes generate a cryptographic **PoQE Attestation Package**—comprising either the D-Wave 64-bit hyperplane witness hash \mathcal{H}(\mathcal{M}) with confidence metadata (\sig[span_94](start_span)[span_94](end_span)ma_W \le 0.16) or the Equal1 RacQ CryoCMOS execution log and Q-CTRL calibration state signed by the rack HSM. The HQCA Gateway aggregates multiple PoQE packages into a single STARK validity proof and anchors the state root to an Ethereum-compatible L1/L2 ledger via an EIP-8141

Frame Transaction.

B. Heterogeneous Workload Partitioning (Resolution of the Cross-Modality Paradox)

A core contribution of the Q-Fabric architecture is the formal resolution of the cross-modality paradox that undermined earlier quantum blockchain proposals. In D-Wave's PoQW protocol (arXiv:2503.14462v3), consensus security rests on **Property 7 (Spoof Resistance)**: generating the expected witness vector W(\rho_\mathcal{M}) must be computationally infeasible for classical computers with realistic resources. D-Wave satisfies this condition by evolving a 3D spin-glass Hamiltonian across thousands of entangled superconducting qubits in the coherent regime.

Conversely, an Equal1 RacQ processor contains N_Q = 6 physical silicon-spin qubits. The pure state |\psi\rangle of a 6-qubit register is fully described by a complex vector in a Hilbert space of dimension:

\dim(\mathcal{H}) = 2^6 = 64

and its density matrix \rho requires only 64 \tim[span_227](start_span)[span_227](end_span)[span_228](start_span)[span_228](end_span)es 64 = 4,096 complex entries. A standard classical CPU or mobile processor can compute exact matrix-vector multiplications on a 64-dimensional state vector in microseconds. Even if an enterprise arrayed K = 1,000 independent RacQ units in parallel without quantum optical interconnects, the composite state space scales additively (1,000 \times 2^6 = 64,000 amplitudes) rather than exponentially (2^{6000}), remaining trivially simulable on a single classical server. Therefore, using 6-qubit gate processors to mine PoQW hashes allows classical ASIC/GPU adversaries to spoof quantum work at negligible cost, while attempting to inject private hardware quantum random numbers into PoQW Step (i) (\Theta = \text{Random}(\mathcal{M})) breaks deterministic Hamiltonian reconstruction across validators.

By abandoning cross-hardware PoQW mining and implementing **Heterogeneous Workload Partitioning**, Q-Fabric utilizes each quantum modality strictly within its physical regime of advantage:

Workload Characteristic	Routed Target: Equal1 RacQ (On-Premise 42U HQCC)	Routed Target: D-Wave Advantage2 (Zephyr-12 Cloud/On-Prem)
Computational Paradigm	Gate-model variational quantum-classical loops (NISQ / CryoCMOS sandbox).	Continuous-time coherent quantum annealing & nonlinear hybrid optimization.
Qubit & Variable Scale	6 physical silicon-spin qubits (linear nearest-neighbor array, 35 CMOS cells).	4,400+ physical superconducting qubits (20-way Zephyr); up to 2M hybrid variables.
Execution Speed & Latency	140 ns (1Q) / 200 ns (2Q); 10,000–100,000 shots/sec; <1\text{ ms} rack loop latency.	5 ns minimum anneal floor; \sim 20.5\ \mu\text{s} QPU delay per sample; 600 reads in <1\text{ s}.
Data Sovereignty Profile	**Strict Sovereign / Air-Gapped:** Data remains inside the local Dell/Equal1	**Cloud or Dedicated Consortium:** Accessed via PQC-encrypted Leap SAPI or

Workload Characteristic	Routed Target: Equal1 RacQ (On-Premise 42U HQCC)	Routed Target: D-Wave Advantage2 (Zephyr-12 Cloud/On-Prem)
	rack.	dedicated QPU.
Target Enterprise Use Cases	Compact molecular chemistry, geometric entanglement estimation (high-order power method), variational feature selection, sovereign HQCC toolchain development.	Supply chain routing, power grid balancing, portfolio tail-risk optimization, 3D spin-glass simulation, verifiable PoQE state auditing.

C. Sovereign Quantum-AI Acceleration and Variational Subroutines

As demonstrated by 2026 evaluations of decentralized Proof of Useful Work (PoUW) networks, attempting to secure a public permissionless blockchain using machine learning training or inference introduces intractable verification asymmetries, replay vulnerabilities, and network latency penalties that negate cryogenic QPU speed. Q-Fabric eliminates speculative public token mining and repositions quantum-AI integration around **Sovereign In-Rack Hybrid Subroutines**.

Within the Equal1 RacQ and Dell PowerEdge R770 rack environment, classical deep learning pipelines running on enterprise GPUs interact natively with the UnityQ QPU across high-speed local interconnects. In these workflows, the classical server performs high-dimensional data ingestion, dimensionality reduction, and gradient aggregation, while offloading specialized subroutines—such as Equal1's published quantum implementation of the high-order power method for estimating geometric entanglement of pure states, kernel matrix estimation, compact combinatorial feature selection, and high-dimensional probability sampling—to the 6-qubit silicon array at 10,000 to 100,000 shots per second. For multi-institution collaborations such as multi-center healthcare or financial fraud consortiums, Q-Fabric supports **Post-Quantum Federated Learning (PQ-FL)**: participating data centers train local hybrid models on their sovereign RacQ/PowerEdge stacks and exchange only FIPS 203 (ML-KEM) encrypted, FIPS 204 (ML-DSA) signed gradient updates, accompanied by PoQE hardware execution attestations.

D. Native Post-Quantum Settlement and Interoperability Framework

Instead of relying on a centralized Web2 API bridge that accepts vulnerable classical ECDSA signatures and relays them to an external blockchain, Q-Fabric aligns directly with the native 2026–2029 post-quantum execution roadmaps of leading Layer-1 smart contract platforms. Following the formation of the Ethereum Foundation's Post-Quantum Security team in January 2026 and the publication of Ethereum's formal PQ roadmap in February 2026, Ethereum has structured a multi-fork migration path toward full L1 quantum resilience by approximately 2029. Building upon the 2025 Pectra (EIP-7702) and Fusaka upgrades and the 2026 Glamsterdam hard fork—which introduces enshrined Proposer-Builder Separation (ePBS, EIP-7732) and mandatory block-level access lists (EIP-7928) to raise execution capacity and parallelize disk reads—Ethereum's 2027 **Hegotá** upgrade is slated to implement Fork-Choice Enforced Inclusion Lists (FOCIL, EIP-7805), Secondary Signature Support (EIP-7932), and **Frame Transactions (EIP-8141)**.

Q-Fabric utilizes EIP-8141 Frame Transactions and ERC-4337 modular smart accounts as its

primary on-chain settlement mechanism:

1. **Native Signature Agility via Frame Transactions (EIP-8141):** Rather than hardcoding secp256k1 ECDSA verification into protocol consensus, EIP-8141 allows each account to define arbitrary validation frames natively at the protocol layer. Q-Fabric enterprise accounts enforce hybrid validation policies (ECDSA + SPHINCS+ or ML-DSA-65) on current testnets and weekly PQ interop devnets, supplemented by ephemeral key rotation commitments (rotating the authorizing signer hash after every transaction to eliminate long-term public key exposure on-chain).
2. **STARK-Based Batch Signature and PoQE Verification:** Because post-quantum signatures require 2,420 to 4,627 bytes for ML-DSA and tens of kilobytes for SLH-DSA (SPHINCS+), verifying dozens of individual PQ signatures directly on-chain strains block gas limits. Adopting the batch verification architecture detailed in Circle's 2026 Post-Quantum Security Roadmap, the Q-Fabric HQCA Gateway aggregates hundreds of ML-DSA workload signatures and D-Wave/RacQ PoQE witness checks off-chain, generates a single post-quantum **STARK (Scalable Transparent Argument of Knowledge)** validity proof, and submits one EIP-8141 transaction to the settlement contract for constant-overhead verification.
3. **Cross-Chain PQ Compatibility:** Beyond Ethereum, Q-Fabric's settlement adapter supports Monad's *Flexible Authentication* standard (allowing existing accounts to retire classical signing authority in place without altering DeFi contract addresses), Algorand's 2027 quantum-resilient state proofs, and Ripple's 2028 XRPL post-quantum signature transition.

IV. HQCA Gateway API Design and Protocol Specification (Formerly C2Q API)

A. Security, Transport, and Cryptographic Requirements

The **HQCA (Hybrid Quantum-Classical Attestation) Gateway API** replaces the legacy HTTP REST interface with a high-throughput, dual-protocol (HTTP/3 REST + gRPC over TLS 1.3) enterprise control plane. Every client connection must negotiate a mutually authenticated TLS 1.3 session using **FIPS 203 (ML-KEM-768)** hybrid key exchange (paired with HQC / FIPS 207 upon 2027 standardization). Every API request mutating state or dispatching compute workloads must include an X-HQCA-PQC-Signature header containing a base64-encoded **FIPS 204 (ML-DSA-65)** digital signature (3,309 bytes raw) computed over the canonicalized payload and a monotonic nonce, verified by the gateway using CMVP-validated cryptographic libraries.

B. Production v2 Endpoint Specification

Endpoint Path	Method / Protocol	Functional Description	Request Payload / Parameters	Response Payload (JSON / Protobuf)
/api/v2/workloads/dispatch	POST (gRPC / REST)	Dispatches a hybrid quantum-classical workload to the Dell Quantum	workloadType (VARIATIONAL_SHOTS | SPIN_GLASS_OPT), sovereigntyTier	jobId, assignedTarget (EQUAL1_RACQ_LOCAL | DWAVE_ADV2_Z1

Endpoint Path	Method / Protocol	Functional Description	Request Payload / Parameters	Response Payload (JSON / Protobuf)
		Intelligent Orchestrator for routing to Equal1 RacQ or D-Wave Advantage2.	(AIR_GAPPED_RACK | CLOUD_ANNEAL), circuitOrHamiltonian, mlDsa65Signature (3,309 B).	2), estimat[span_275](start_span)[span_275](end_span)[span_276](start_span)[span_276](end_span)edLatencyMs, pqcReceiptHash.
/api/v2/attestation/witness/{jobId}	GET (gRPC / REST)	Retrieves the cryptographic Proof of Quantum Execution (PoQE) package and computational output for a completed job.	jobId (path parameter), incl[span_280](start_span)[span_280](end_span)[span_281](start_span)[span_281](end_span)udeRawSamples (query boolean).	solutionVector, poqeType (HYPERPLANE_WITNESS_V3 | CRYOCMOS_HSM_LOG), witnessHash64Bit, witnessUncertainty ($\sigma_W \le 0.[span_282](start_span)[span_282](end_span)[span_283](start_span)[span_283](end_span)[span_284](start_span)[span_284](end_span)1), hamiltonianScaleFactor.
/api/v2/telemetry/rack/{rackId}	GET (gRPC Stream)	Streams real-time hardware health, cryocooler telemetry, and Q-CTRL autocalibration metrics from the co-located 42U HQCC rack.	rackId (path parameter).	cryoTempKelvin (0.30), coolingPowerUw (160), powerDrawWatts (1600), fidelity1Q (0.999), fidelity2Q (0.993), swapTax6Q (0.912), serviceHoursRemaining.
/api/v2/settlement/anchor	POST (gRPC / REST)	Aggregates verified PoQE packages into a STARK batch proof and anchors the state root	jobIds[], targetNetwork (ETHEREUM_HEGOTA_DEVNET | MONAD_PQ), accountFramePoli	batchStarkProofHash, eip8141TxHash, aggregatedSignaturesCount, gasSavedBytes.

Endpoint Path	Method / Protocol	Functional Description	Request Payload / Parameters	Response Payload (JSON / Protobuf)
		on-chain via an EIP-8141 Frame Transaction.	cy (ML_DSA_65 | SPHINCS_HYBRID).	

V. Reference Implementation and Conceptual Code Architecture

The following conceptual Python reference implementations supersede the deprecated 2025 code modules. They illustrate the four core pillars of the Q-Fabric architecture: (1) FIPS 204 ML-DSA-65 workload dispatch, (2) Equal1 RacQ SWAP-aware circuit transpilation on the 6-qubit linear array, (3) D-Wave Advantage2 Proof of Quantum Execution (PoQE) hyperplane witness validation (arXiv:2503.14462v3), and (4) STARK-batched EIP-8141[span_288](start_span)[span_288](end_span)[span_289](start_span)[span_289](end_span)[span_290](start_span)[span_290](end_span)[span_291](start_span)[span_291](end_span)[span_292](start_span)[span_292](end_span)[span_293](start_span)[span_293](end_span) Frame Transaction settlement.

```
import hashlib
import json
import numpy as np
from dataclasses import dataclass,
[span_99](start_span)[span_99](end_span)asdict
from typing import Dict, List, Tuple

#
================================================================
======
# MODULE 1: Equal1 RacQ 6-Qubit Linear Array
SWAP-Awar[span_100](start_span)[span_100](end_span)e Transpiler &
Runner
# Enforces GlobalFoundries 22FDX UnityQ linear topology and models 2Q
SWAP tax
#
================================================================
======

@dataclass
class RacQTelemetry:
    rack_id: str = "DELL-R770-RACQ-42U-01"
    cryo_temp_kelvin: float = 0.30
    power_consumption_watts: int = 1600
    f_1q_avg: float = 0.999       # 140 ns randomized Clifford
    f_2q_nearest: float = 0.993   # 200 ns interleaved benchmarking
    readout_fidelity: float = 0.999
    readout_time_us: float = 10.0
    service_interval_hrs_remaining: int = 4820
```

```
class Equal1RacQAccelerator:
    """Simulates co-located Equal1 RacQ execution with linear SWAP
routing audit."""
    def __init__(self):
        self.num_qubits = 6
        self.telemetry = RacQTelemetry()

    def calculate_routing_fidelity(self, qubit_a: int, qubit_b: int)
-> Tuple[float, float, int]:
        """
        Computes effective 2Q fidelity and gate duration across the
6-qubit linear chain.
        Each SWAP requires 3 CNOTs. Entangling Q1 (idx 0) and Q6 (idx
5) requires 4 SWAPs
        (12 CNOTs + 1 target gate = 13 two-qubit operations ->
0.993^13 = 91.2% fidelity).
        """
        if not (0 <= qubit_a < self.num_qubits and 0 <= qubit_b <
self.num_qubits):
            raise ValueError("Qubit index out of bounds for 6-qubit
UnityQ linear array.")
        distance = abs(qubit_a - qubit_b)
        if distance == 0:
            return 1.0, 0.0, 0
        num_swaps = distance - 1
        total_2q_gates = (3 * num_swaps) + 1
        effective_fidelity = self.telemetry.f_2q_nearest **
total_2q_gates
        duration_ns = total_2q_gates * 200.0
        return round(effective_fidelity, 4), duration_ns, num_swaps

    def execute_variational_subroutine(self, circuit_edges:
List[Tuple[int, int]], shots: int = 50000) -> Dict:
        """Executes high-speed variational loop (10k-100k shots/sec)
with CryoCMOS attestation."""
        cumulative_fidelity = 1.0
        total_duration_ns = 0.0
        total_swaps = 0

        for q_a, q_b in circuit_edges:
            f_eff, dur_ns, swaps =
self.calculate_routing_fidelity(q_a, q_b)
            cumulative_fidelity *= f_eff
            total_duration_ns += dur_ns
            total_swaps += swaps

        # Deterministic mock parity readout expectation values for
```

```
6-qubit subroutine
        rng = np.random.default_rng(seed=len(circuit_edges) + shots)
        parity_expectations = rng.uniform(-1.0, 1.0,
size=self.num_qubits).round(5).tolist()

        return {
            "target": "EQUAL1_RACQ_UNITYQ_22FDX",
            "shots_executed": shots,
            "total_swaps_incurred": total_swaps,
            "estimated_circuit_fidelity": round(cumulative_fidelity,
4),
            "gate_execution_time_us": round(total_duration_ns /
1000.0, 3),
            "parity_observables": parity_expectations,
            "telemetry_snapshot": asdict(self.telemetry)
        }


#
================================================================================
======
# MODULE 2: D-Wave Advantage2 Proof of Quantum Execution (PoQE) Engine
# Implements arXiv:2503.14462v3 Hyperplane Witness Discretization &
Validation
#
================================================================================
======

class DWaveAdvantage2PoQE:
    """
    Implements verifiable Proof of Quantum Execution (PoQE) on 4,400+
qubit Zephyr-12
    spin-glass Hamiltonians with 64-bit hyperplane witness
discretization.
    """
    HASH_BITS = 64
    DEFAULT_NUM_READS = 600
    CALIBRATED_WITNESS_UNCERTAINTY = 0.16  # Jan 2026 Advantage2
benchmark baseline
    MIN_ANNEAL_TIME_NS = 5.0

    @staticmethod
    def preprocess_message_to_couplings(workload_id: str, nonce: int)
-> np.ndarray:
        """
        Step (i) Preprocessing: Transform workload message M into
deterministic coupler
        parameters Theta = Random(M) with h_i = 0, J_ij = Theta(M).
```

```
Excludes wall timestamp.
        """
        seed_bytes =
hashlib.sha3_256(f"{workload_id}:{nonce}".encode("utf-8")).digest()
        seed_int = int.from_bytes(seed_bytes[:8], "big")
        rng = np.random.default_rng(seed_int)
        return rng.uniform(-1.0, 1.0,
size=DWaveAdvantage2PoQE.HASH_BITS)

    @classmethod
    def generate_poqe_witness(cls, workload_id: str, nonce: int,
energy_scale_ratio: float = 1.40) -> Dict:
        """
        Steps (ii)-(iv): Simulates unitary evolution with Advantage2
Hamiltonian rescaling,
        computes 64 observable witnesses W_alpha across 600 reads, and
discretizes via Heaviside.
        """
        # Rescale Hamiltonian down if QPU energy scale exceeds
prototype schedule (+40% on Adv2)
        hamiltonian_rescale = 1.0 / energy_scale_ratio if
energy_scale_ratio > 1.0 else 1.0
        couplings = cls.preprocess_message_to_couplings(workload_id,
nonce) * hamiltonian_rescale

        # Simulate expected observable witness vector W(rho_M) with
cross-QPU sampling noise
        rng = np.random.default_rng(abs(hash(workload_id)) % (2**32))
        sampling_noise = rng.normal(0.0,
cls.CALIBRATED_WITNESS_UNCERTAINTY / np.sqrt(cls.DEFAULT_NUM_READS),
size=cls.HASH_BITS)
        witness_vector = np.tanh(couplings) + sampling_noise

        # Step (iv) Digitalization: H_alpha = theta(W_alpha -
W_0_alpha) where W_0_alpha = 0.0
        binary_bits = (witness_vector >= 0.0).astype(int)
        quantum_hash_str = "".join(map(str, binary_bits.tolist()))

        return {
            "solver": "Advantage2_system1_Zephyr12",
            "num_reads": cls.DEFAULT_NUM_READS,
            "hamiltonian_rescale_factor": round(hamiltonian_rescale,
4),
            "witness_vector": witness_vector.round(5).tolist(),
            "quantum_witness_hash_64b": quantum_hash_str,
            "witness_uncertainty_sigma":
cls.CALIBRATED_WITNESS_UNCERTAINTY
        }
```

```
    @classmethod
    def validate_poqe_probabilistic(cls, miner_witness_hash: str,
validator_witness_vec: List[float]) -> Dict:
        """
        Probabilistic Validation: Evaluates received 64-bit quantum
hash against validator's
        observed witness distances from hyperplane W_0 = 0.0.
        """
        miner_bits = [int(b) for b in miner_witness_hash]
        mismatches = 0
        log_confidence_penalty = 0.0

        for bit, w_val in zip(miner_bits, validator_witness_vec):
            val_bit = 1 if w_val >= 0.0 else 0
            # Probability of bit stability increases with distance
from hyperplane W_0 = 0
            distance_z = abs(w_val) /
cls.CALIBRATED_WITNESS_UNCERTAINTY
            p_alpha = float(np.clip(0.5 + 0.5 * np.tanh(distance_z),
0.5001, 0.9999))

            if bit != val_bit:
                mismatches += 1
                # Confidence decreases by factor (1 - P_alpha) /
P_alpha on mismatch
                penalty_factor = (1.0 - p_alpha) / p_alpha
                log_confidence_penalty += np.log10(penalty_factor)

        is_valid = mismatches <= 2 and log_confidence_penalty > -1.5
        return {
            "poqe_verified": bool(is_valid),
            "bit_mismatches": mismatches,
            "log10_confidence_score":
round(float(log_confidence_penalty), 4)
        }


#
================================================================
======
# MODULE 3: HQCA Gateway Controller & EIP-8141 STARK Settlement Anchor
# Enforces FIPS 204 ML-DSA-65 (3,309-byte) signatures & STARK batch
anchoring
#
================================================================
======
```

```
class HQCAGatewayController:
    FIPS_204_ML_DSA_65_SIG_BYTES = 3309

    def __init__(self):
        self.racq = Equal1RacQAccelerator()
        self.attestation_pool: List[Dict] = []

    def dispatch_hybrid_workload(self, payload: Dict, ml_dsa_65_sig:
bytes) -> Dict:
        """Validates FIPS 204 ML-DSA-65 signature size and routes via
Dell Orchestrator logic."""
        if len(ml_dsa_65_sig) != self.FIPS_204_ML_DSA_65_SIG_BYTES:
            raise PermissionError(
                f"Rejected: FIPS 204 ML-DSA-65 signature must be
exactly {self.FIPS_204_ML_DSA_65_SIG_BYTES} bytes."
            )

        workload_type = payload.get("workloadType")
        if workload_type == "VARIATIONAL_SHOTS":
            result = self.racq.execute_variational_subroutine(
                circuit_edges=payload.get("circuitEdges", [(0, 1), (1,
2), (2, 3)]),
                shots=payload.get("shots", 50000)
            )
        elif workload_type == "SPIN_GLASS_OPT":
            result = DWaveAdvantage2PoQE.generate_poqe_witness(
                workload_id=payload["workloadId"],
                nonce=payload.get("nonce", 42)
            )
        else:
            raise ValueError("Unsupported workloadType.")

        attestation_record = {
            "workloadId": payload["workloadId"],
            "pqcAlgorithm": "NIST-FIPS-204-ML-DSA-65",
            "executionResult": result
        }
        self.attestation_pool.append(attestation_record)
        return attestation_record

    def anchor_stark_batch_eip8141(self) -> Dict:
        """
        Compresses pending PoQE attestations and 3,309-byte ML-DSA-65
signatures into a
        single STARK proof for an Ethereum EIP-8141 Frame Transaction.
        """
        batch_count = len(self.attestation_pool)
        raw_sig_bytes = batch_count *
```

```
self.FIPS_204_ML_DSA_65_SIG_BYTES
        serialized_batch = json.dumps(self.attestation_pool,
sort_keys=True).encode("utf-8")
        stark_proof_commitment =
hashlib.sha3_256(serialized_batch).hexdigest()

        eip8141_frame_tx = {
            "txType": "0x06_EIP8141_FRAME_TX",
            "targetFork": "Ethereum_Hegota_2027_Interop",
            "validationFramePolicy":
"STARK_BATCHED_ML_DSA_65_AND_SPHINCS_FALLBACK",
            "aggregatedJobsCount": batch_count,
            "uncompressedSignatureOverheadBytes": raw_sig_bytes,
            "starkProofCommitment": f"0x{stark_proof_commitment}",
            "ephemeralSignerRotationCommitment":
f"0x{hashlib.sha3_256(stark_proof_commitment.encode()).hexdigest()[:40
]}"
        }
        self.attestation_pool.clear()
        return eip8141_frame_tx

if __name__ == "__main__":
    gateway = HQCAGatewayController()
    mock_ml_dsa_65_sig = b"\xfa" * 3309  # Exact FIPS 204 ML-DSA-65
byte footprint

    # 1. Dispatch sovereign variational loop to in-rack Equal1 RacQ
    racq_job = gateway.dispatch_hybrid_workload(
        {"workloadId": "ESA-EO-VARIATIONAL-01", "workloadType":
"VARIATIONAL_SHOTS", "circuitEdges": [(0, 1), (1, 2)]},
        mock_ml_dsa_65_sig
    )
    # 2. Dispatch combinatorial spin-glass optimization to D-Wave
Advantage2
    dwave_job = gateway.dispatch_hybrid_workload(
        {"workloadId": "PORTFOLIO-TAIL-RISK-99", "workloadType":
"SPIN_GLASS_OPT", "nonce": 202610},
        mock_ml_dsa_65_sig
    )
    # 3. Anchor batch via STARK-compressed EIP-8141 Frame Transaction
    settlement_receipt = gateway.anchor_stark_batch_eip8141()
    print(json.dumps(settlement_receipt, indent=2))
```

VI. Enterprise Feasibility, Economics, and Risk Analysis

A. Capital, Operational, and Cryptographic Attack Economics

Evaluating the financial viability of Q-Fabric requires comparing the capital and operational expenditure (CapEx/OpEx) of on-premise HQCC infrastructure against both traditional cryogenic facilities and the modeled economic threat of quantum key-recovery attacks:

1. **Data Center Infrastructure Economics:** First-generation superconducting quantum systems require specialized vibration-isolated rooms, external dilution refrigeration, liquid helium supply chains, and ~25 kW of electrical power. Conversely, the Equal1 RacQ server installs directly into an existing 42U data center frame alongside a Dell PowerEdge R770 server, operates on 1,600 W from a standard 208/240V 16A single-phase outlet, and runs continuously for 5,000 hours between sorption cooler maintenance intervals. More importantly, because UnityQ is fabricated on commercial 22FDX CMOS silicon and designed around a modular QPU tile upgrade path, enterprises preserve 100% of their rack, cooling, power, and orchestration CapEx across successive hardware generations—compounding computational capability in place.
2. **Asymmetric Quantum Attack Economics:** As modeled in Monad's 2026 Post-Quantum Security analysis, even if a cryptanalytically relevant quantum computer carries a capital cost of 38.9 billion over a five-year useful life at a 50% productive utilization ratio (1,314,000$ operating minutes), an 18-to-23-minute Shor's key recovery attack carries an amortized capital cost of approximately **$530,000 to $680,000 per run**. Because the quantum machine can be reused indefinitely across high-value targets, any enterprise treasury, cross-chain bridge, or institutional wallet holding over $1 million secured by exposed classical ECDSA keys faces an economically rational existential threat. Migrating to Q-Fabric's FIPS 204 ML-DSA and Ethereum EIP-8141 Frame Transaction architecture eliminates this vulnerability prior to CRQC deployment.

B. Regulatory Compliance and Data Sovereignty

The regulatory environment governing cryptographic infrastructure tightened decisively in mid-2026. Under **OMB Memorandum M-26-15** (June 24, 2026), the **June 2026 Executive Order** on CMVP module validation, and **NSA National Security System mandates** requiring PQC adoption across software/firmware signing, TLS cloud services, and traditional network equipment in 2025–2026 ahead of the 2035 federal cutoff, enterprises operating hybrid cloud architectures must demonstrate verifiable crypto-agility. Q-Fabric satisfies these mandates natively by enforcing CMVP-validated FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) primitives today, while pre-allocating protocol buffer capacity for FIPS 207 (HQC) in 2027. Simultaneously, for defense, sovereign wealth, and aerospace entities bound by strict territorial data residency laws, RacQ's co-located rack execution ensures that sensitive training weights and optimization inputs never traverse external public networks.

C. Multi-Phase Hardware Scaling Roadmap

Q-Fabric's hardware lifecycle is synchronized with Equal1's three-phase silicon scaling trajectory and D-Wave's annealing roadmap:

- **Phase 1: NISQ & First In-Rack Hybrid Workloads (2025–2026 — Current Production):** Deployment of the 6-qubit Equal1 RacQ server co-located with Dell PowerEdge R770 and Q-CTRL autonomous calibration for high-shot-rate variational

sampling, compact molecular chemistry, and HQCC orchestration testing, paired with D-Wave Advantage2 (4,400+ qubits) for production combinatorial optimization and PoQE state attestation.
- **Phase 2: Early Fault-Tolerant Multi-Tile QSoC (2027–2029):** In-place field upgrades of the RacQ QPU module leveraging repeatable UnityQ CMOS tiles with deeper CryoCMOS real-time error correction code distances, enabling actionable molecular structure, battery catalyst, and drug discovery simulations alongside Ethereum's 2027 Hegotá (EIP-8141) and 2029 L1 post-quantum completion milestones.
- **Phase 3: Fully Fault-Tolerant Post-Classical Infrastructure (2030–2035):** Scaling to millions of physical silicon-spin qubits and thousands of logical qubits within the same 42U data center rack footprint, achieving full post-classical production compute ahead of the 2035 federal PQC transition deadline.

VII. Conclusion and Strategic Summary

By evolving from the speculative March 2025 C2Q cryptocurrency mining proposal into the **Q-Fabric Sovereign Hybrid Quantum-Classical Orchestration and Attestation Platform**, enterprise architects eliminate the physical impossibility of cross-modality 6-qubit PoQW mining and the security exposure of classical-signature bridges. Grounded in October 2026 production technology—combining co-located **Equal1 RacQ (UnityQ 22FDX CMOS)** and **Dell PowerEdge R770** rack systems, **D-Wave Advantage2 (Zephyr-12)** coherent annealers, **Proof of Quantum Execution (PoQE)** hyperplane witness auditing (arXiv:2503.14462v3), **NIST FIPS 203/204/205/207** cryptography, and **Ethereum EIP-8141** STARK-batched settlement—Q-Fabric delivers an actionable, compliant, and future-proof foundation for the post-quantum enterprise.

VIII. Works Cited and Authoritative References

A. Equal1 Silicon-Spin Hardware, Bell-1, and RacQ HQCC Architecture

1. Equal1. "Equal1 Launches Bell-1: The First Quantum System Purpose-Built for the HPC Era." *Equal1 Insights*, March 16, 2025. https://www.equal1.com/insights/equal1-launches-bell-1-the-first-quantum-system-purpose-built-for-the-hpc-era.
2. TechPowerUp. "Equal1 Launches Bell-1: The First Quantum System Purpose-Built for the HPC Era." March 17, 2025. https://www.techpowerup.com/334197/equal1-launches-bell-1-the-first-quantum-system-purpose-built-for-the-hpc-era.
3. Choucair, Cierra. "Equal1 Introduces Bell-1: A Rack-Mountable Quantum System for HPC Environments." *The Quantum Insider*, March 17, 2025. https://thequantuminsider.com/2025/03/17/equal1-introduces-bell-1-a-rack-mountable-quantum-system-for-hpc-environments/.
4. Quantum Computing Report. "Equal1 Launches Bell-1, 6-qubit Silicon-Based Quantum Server for HPC Environments." March 2025. https://quantumcomputingreport.com/equal1-launches-bell-1-6-qubit-silicon-based-quantum-server-for-hpc-environments/.
5. Alaka, Solomon. "The Quantum Standard: NovaUCD Equal1 Secures $60M to Deploy World's First Data Centre-Ready Quantum Server." *The News Intel*, January 16, 2026.

https://thenewsintel.com/the-quantum-standard-novaucd-equal1-secures-60m-to-deploy-worlds-first-data-centre-ready-quantum-server/.
6. Q-CTRL & Equal1. "Equal1 and Q-CTRL Partner to Deliver Fully Autonomous, Data Center-Ready Quantum Computing." *Q-CTRL Technical Blog*, April 8, 2026. https://q-ctrl.com/blog/equal1-and-q-ctrl-partner-to-deliver-fully-autonomous-data-center-ready-quantum-computing.
7. Equal1. "Equal1 Unveils World's First Hybrid Rack-Mounted Silicon-Spin Quantum Computer (RacQ)." *Equal1 Insights*, May 14, 2026. https://www.equal1.com/insights/equal1-unveils-worlds-first-hybrid-rack-mounted-silicon-spin-quantum-computer.
8. Quantum Computing Report. "Equal1 Unveils Rack-Mounted Silicon-Spin Quantum Computer." May 15, 2026. https://quantumcomputingreport.com/equal1-unveils-rack-mounted-silicon-spin-quantum-computer/.
9. Equal1. "Equal1 RacQ Product Specifications & System Architecture." Accessed October 2026. https://www.equal1.com/product.
10. Equal1. "UnityQ Technology: CryoCMOS and Commercial 22FDX Silicon Spin Qubits." Accessed October 2026. https://www.equal1.com/technology.
11. Equal1. "Equal1 Hardware Scaling Roadmap: NISQ to Fault-Tolerant In-Rack Compute." Accessed October 2026. https://www.equal1.com/roadmap.
12. Dell Technologies. "Driving Quantum Innovation with Dell Infrastructure: Dell PowerEdge R770, PowerSwitch, and Quantum Intelligent Orchestrator with Equal1 RacQ." Accessed October 2026. https://www.dell.com/en-us/learn/it-infrastructure/lp/workload-solutions/workloads-quantum-computing.
13. Firebringer Quantum. "Equal1's RacQ Silicon-Spin Rack Quantum Computer: 22FDX CMOS, CryoCMOS Control, and Linear SWAP Routing Analysis." 2026. https://firebringerquantum.com/blog/equal1-racq-silicon-spin-rack-quantum-computer.html.
14. DataCenterDynamics (DCD). "European Space Agency to Install Equal1 Bell-1 Quantum Computer for Earth Observation Data Processing." July 2026. https://www.datacenterdynamics.com/en/news/european-space-agency-to-install-equal1-bell-1-quantum-computer-for-earth-observation-data-processing/.
15. DataCenterDynamics (DCD). "Equal1 Unveils Rack-Mounted Silicon-Spin Quantum Computer, RacQ." May 2026. https://www.datacenterdynamics.com/en/news/equal1-unveils-rack-mounted-silicon-spin-quantum-computer-racq/.

B. D-Wave Quantum Annealing, Advantage2 (Zephyr-12), and Verifiable Quantum Work

1. Amin, Mohammad H., Jack Raymond, Daniel Kinn, Gunnar Miller, Firas Hamze, Kelsey Hamer, Joel Pasvolsky, William Bernoudy, Andrew D. King, and Samuel Kortas. "Blockchain with proof of quantum work." *arXiv preprint arXiv:2503.14462v3 [quant-ph]*, submitted March 18, 2025, last revised February 9, 2026. https://arxiv.org/abs/2503.14462 and https://arxiv.org/html/2503.14462v3.
2. D-Wave Systems Inc. "Blockchain with Proof of Quantum Work: Reference Simulation

and Advantage2 Calibration (dwave-examples/quantum-blockchain)." *GitHub Repository*, updated 2026. https://github.com/dwave-examples/quantum-blockchain.
3. D-Wave Quantum Inc. "D-Wave Announces General Availability of Advantage2 Quantum Computer, Its Most Advanced and Performant System." *Press Release*, May 20, 2025. https://www.dwavequantum.com/company/newsroom/press-release/d-wave-announces-general-availability-of-advantage2-quantum-computer-its-most-advanced-and-performant-system/.
4. D-Wave Quantum Inc. "Performance Gains in the D-Wave Advantage2 System at the 4,400-Qubit Scale (Zephyr-12 Whitepaper)." *D-Wave Technical Report 14-1083A-A*, May 2025. https://www.dwavequantum.com/media/wakjcpsf/adv2_4400q_whitepaper-1.pdf.
5. D-Wave Quantum Inc. "Leap SAPI Release Notes & Per-QPU Solver Properties and Schedules (Advantage2_system1, Advantage2_system2, Advantage2_system4)." Updated October 27, 2026. https://docs.dwavequantum.com/projects/leap_sapi/en/latest/release_notes.html and https://docs.dwavequantum.com/en/latest/quantum_research/solver_properties_specific.html.
6. D-Wave Quantum Inc. "D-Wave Delivers Italy's First Annealing Quantum Computer (Advantage2)." *Nasdaq Press Release*, October 15, 2026. https://www.nasdaq.com/press-release/d-wave-delivers-italys-first-annealing-quantum-computer-2026-10-15.
7. Quantum Computing Report. "2026 Quantum News Archive: D-Wave Advantage2 Ledger Verification and Error-Aware Gate-Model Simulator." June 2026. https://quantumcomputingreport.com/news-archive-2026/.

C. NIST Post-Quantum Cryptography (PQC) Standards and Federal Directives

1. National Institute of Standards and Technology (NIST). "NIST Releases First 3 Finalized Post-Quantum Encryption Standards (FIPS 203, FIPS 204, FIPS 205)." August 13, 2024. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.
2. National Institute of Standards and Technology (NIST). "Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process (Selection of HQC)." *NIST IR 8545*, March 11, 2025. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.
3. Moody, Dustin (NIST). "NIST PQC: The Road Ahead (Round 4 HQC Selection, ISO Standardization, and 2035 Migration Target)." *NIST PQC Presentation*, 2025. https://csrc.nist.gov/csrc/media/presentations/2025/nist-pqc-project/nist_pqc_the_road_ahead-moody_1.1.pdf.
4. Perlner, Ray (NIST). "FIPS 206: FN-DSA (FALCON) — Floating-Point Validation Challenges and Planned Changes." *NIST PQC Presentation*, 2025. https://csrc.nist.gov/csrc/media/presentations/2025/fips-206-fn-dsa-(falcon)/images-media/fips_206-perlner_2.1.pdf.
5. Kelly, Shane. "Quantum-Ready FN-DSA (FIPS 206) Nears Draft Approval from NIST." *DigiCert PQC Blog*, September 5, 2025. https://www.digicert.com/blog/quantum-ready-fndsa-nears-draft-approval-from-nist.

6. ArcQubit Team. "NIST PQC Standards Guide: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA), FN-DSA (FIPS 206), HQC, and OMB Memorandum M-26-15." *ArcQubit*, updated September 30, 2026. https://www.arcqubit.ai/blog/nist-pqc-standards-guide.
7. Quantum Sequrity. "NIST Round 4 KEM Candidates: Final Status (HQC on FIPS 207 Track, Classic McEliece, and BIKE)." Updated October 2026. https://quantumsequrity.com/blog/nist-round-4-status.
8. IEEE / NSF Public Access Repository. "Post-Quantum Cryptography Ecosystem Readiness, NSA NSS 2025–2035 Mandates, and OpenSSL PQC Integration." Accessed May 2026. https://par.nsf.gov/servlets/purl/10684933.

D. Native Blockchain Post-Quantum Roadmaps, Account Abstraction, and PoUW Analysis

1. Ethereum Foundation. "Ethereum Security & Post-Quantum Resistance Roadmap (Glamsterdam ePBS EIP-7732, Hegotá FOCIL EIP-7805 & Frame Transactions EIP-8141)." *Ethereum.org*, updated mid-2026. https://ethereum.org/roadmap/security/ and https://ethereum.org/roadmap/.
2. Thirdweb Engineering. "Post-Quantum Wallet Security on Ethereum: What Developers Need to Know in 2026 (EIP-8141, EIP-7932, ERC-4337 Hybrid SPHINCS+)." July 30, 2026. https://blog.thirdweb.com/post-quantum-wallet-security-on-ethereum-what-developers-need-to-know-in-2026/.
3. Monad / Category Labs. "Monad's Post-Quantum Roadmap: Flexible Authentication, Quantum Attack Capital Modeling, and Consensus Migration." 2026. https://monad.xyz/blog/post-quantum-roadmap.
4. Circle. "Circle's Post-Quantum Security Roadmap: Securing Blockchains, Smart Contracts, and Digital Assets via STARK Batch Signature Verification." 2026. https://6778953.fs1.hubspotusercontent-na1.net/hubfs/6778953/PDFs/quantum_paper.pdf .
5. Tangem & QuanChain. "Ethereum Post-Quantum Roadmap 2026 (EIP-7702 to Native PQ Signatures)." 2026. https://tangem.com/en/blog/post/post-quantum-cryptography/ and https://www.quanchain.ai/guides/ethereum-post-quantum-roadmap-2026.
6. Simback, Kevin. "Proof of Useful Work: Make Mining Great Again (Architectural Complexities and Verification Limits of PoUW)." June 1, 2026. https://kevinsimback.com/writing/proof-of-useful-work-make-mining-great-again/.
7. Gharavi, H., et al., & Gurung, D., et al. "Post-Quantum Secure Blockchain Federated Learning & Hybrid Blockchain Interoperability." *arXiv / Semantic Scholar*, 2024–2025.

Works cited

1. Quantum One | C2Q Blockchain Architecture, https://quantumone.io/ 2. C2Q - Quantum Blockchain Architecture Proposal.pdf, uploaded:C2Q - Quantum Blockchain Architecture Proposal.pdf 3. Equal1 Unveils World's First Hybrid Rack-Mounted Silicon-Spin, https://www.equal1.com/insights/equal1-unveils-worlds-first-hybrid-rack-mounted-silicon-spin-quantum-computer 4. NIST PQC Standards Guide: FIPS 203, 204, 205 | ArcQubit, https://www.arcqubit.ai/blog/nist-pqc-standards-guide 5. News Archive 2026 - Quantum

Computing Report, https://quantumcomputingreport.com/news-archive-2026/ 6. UnityQ - Equal1, https://www.equal1.com/technology 7. Equal1 Launches Bell-1: The First Quantum System Purpose-Built, https://www.equal1.com/insights/equal1-launches-bell-1-the-first-quantum-system-purpose-built-for-the-hpc-era 8. The Quantum Standard: NovaUCD Equal1 Secures $60M to Deploy, https://thenewsintel.com/the-quantum-standard-novaucd-equal1-secures-60m-to-deploy-worlds-first-data-centre-ready-quantum-server/ 9. Equal1 unveils rack-mounted silicon-spin quantum computer, RacQ, https://www.datacenterdynamics.com/en/news/equal1-unveils-rack-mounted-silicon-spin-quantum-computer-racq/ 10. Equal1 RacQ, https://www.equal1.com/product 11. Equal1's RacQ: A Fab-Compatible Quantum Sandbox, Not a, https://firebringerquantum.com/blog/equal1-racq-silicon-spin-rack-quantum-computer.html 12. D-Wave's Advantage2 Quantum Computer Now Generally Available, https://support.dwavesys.com/hc/en-us/articles/32105885880087-D-Wave-s-Advantage2-Quantum-Computer-Now-Generally-Available 13. Performance gains in the D-Wave Advantage2 system at the 4400, https://www.dwavequantum.com/media/wakjcpsf/adv2_4400q_whitepaper-1.pdf 14. Blockchain with proof of quantum work - arXiv, https://arxiv.org/pdf/2503.14462 15. A proof of quantum work simulated blockchain on D-Wave ... - GitHub, https://github.com/dwave-examples/quantum-blockchain 16. [2503.14462] Blockchain with proof of quantum work - arXiv, https://arxiv.org/abs/2503.14462 17. NIST Post-Quantum Cryptography Standardization - Wikipedia, https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization 18. NIST Round 4 KEM Candidates: Final Status | QNSQY, https://quantumsequrity.com/blog/nist-round-4-status 19. PQC Standardization Process - Post-Quantum Cryptography | CSRC, https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization 20. A Survey of Post-Quantum Cryptography Support in Cryptographic, https://par.nsf.gov/servlets/purl/10684933 21. NIST PQC The Road Ahead, https://csrc.nist.gov/csrc/media/presentations/2025/nist-pqc-project/nist_pqc_the_road_ahead-moody_1.1.pdf 22. Your Guide to Post-Quantum Cryptography (PQC) [2026 Update], https://tangem.com/en/blog/post/post-quantum-cryptography/ 23. A more secure Ethereum, https://ethereum.org/roadmap/security/ 24. Post-Quantum Wallet Security on Ethereum | Developer Guide 2026, https://blog.thirdweb.com/post-quantum-wallet-security-on-ethereum-what-developers-need-to-know-in-2026/ 25. Monad's post-quantum roadmap, https://monad.xyz/blog/post-quantum-roadmap 26. D-Wave Announces General Availability of Advantage2 Quantum, https://www.dwavequantum.com/company/newsroom/press-release/d-wave-announces-general-availability-of-advantage2-quantum-computer-its-most-advanced-and-performant-system/ 27. Quantum Computing Solutions | Dell USA, https://www.dell.com/en-us/learn/it-infrastructure/lp/workload-solutions/workloads-quantum-computing 28. Circle's Post-Quantum Security Roadmap, https://6778953.fs1.hubspotusercontent-na1.net/hubfs/6778953/PDFs/quantum_paper.pdf 29. Equal1 Stock: Private Status, RacQ & Funding (2026) - Quantum, https://quantummarketcap.com/company/equal1 30. ESA Installs Its First On-Premises Quantum Computer to Boost Earth, https://quantumcomputingreport.com/esa-installs-its-first-on-premises-quantum-computer-to-boo

st-earth-observation-capabilities/ 31. Equal1 Introduces Bell-1: A Rack-Mountable Quantum System for,
https://thequantuminsider.com/2025/03/17/equal1-introduces-bell-1-a-rack-mountable-quantum-system-for-hpc-environments/ 32. European Space Agency to install Equal1 Bell-1 quantum computer,
https://www.datacenterdynamics.com/en/news/european-space-agency-to-install-equal1-bell-1-quantum-computer-for-earth-observation-data-processing/ 33. Equal1 and Q-CTRL Partner to Deliver Fully Autonomous, Data,
https://q-ctrl.com/blog/equal1-and-q-ctrl-partner-to-deliver-fully-autonomous-data-center-ready-quantum-computing 34. Per-QPU Solver Properties and Schedules - D-Wave Documentation,
https://docs.dwavequantum.com/en/latest/quantum_research/solver_properties_specific.html 35. Release Notes — Project name not set documentation,
https://docs.dwavequantum.com/projects/leap_sapi/en/latest/release_notes.html 36. D-Wave Delivers Italy's First Annealing Quantum Computer | Nasdaq,
https://www.nasdaq.com/press-release/d-wave-delivers-italys-first-annealing-quantum-computer-2026-10-15 37. Quantum-Ready FN-DSA (FIPS 206) Nears Draft Approval from NIST,
https://www.digicert.com/blog/quantum-ready-fndsa-nears-draft-approval-from-nist 38. FIPS 206 Status Update - NIST Computer Security Resource Center,
https://csrc.nist.gov/csrc/media/presentations/2025/fips-206-fn-dsa-(falcon)/images-media/fips_206-perlner_2.1.pdf 39. Equal1 Unveils Rack-Mounted Silicon-Spin Quantum Computer,
https://quantumcomputingreport.com/equal1-unveils-rack-mounted-silicon-spin-quantum-computer/ 40. Proof of Useful Work: Make Mining Great Again | Kevin Simback,
https://kevinsimback.com/writing/proof-of-useful-work-make-mining-great-again/ 41. Ethereum roadmap | ethereum.org, https://ethereum.org/roadmap/ 42. Ethereum's Post-Quantum Roadmap: Where It Stands in 2026,
https://www.quanchain.ai/guides/ethereum-post-quantum-roadmap-2026 43. Roadmap - Equal1, https://www.equal1.com/roadmap 44. Equal1 | Rack-Mounted Quantum Computers,
https://www.equal1.com/