# World Quantum Computer (WQC) v0.3

### ~ A Decentralized Quantum Simulation Protocol to Shatter Centralized Hegemony ~

## 1. Preface: Rebellion Against Quantum Hegemony (Anti-Hegemony)

### 1.1 The Centralized Quantum Hegemony and Its Threat

Throughout the history of modern computing, the internet and cryptography have served as shields protecting individual sovereignty and privacy. Yet the "dawn of quantum computing" we face today carries an acute crisis of centralization—one that threatens to overturn the decentralized balance of power built over decades.

Developing and operating practical quantum computers (QPUs) requires capital investments on the order of hundreds of billions of yen, dilution refrigerators that maintain millikelvin temperatures, and highly specialized academic teams. These physical and economic constraints have produced an **oligopoly of quantum computing resources** dominated by a handful of nation-states, national-scale technology giants (Big Tech), and military-industrial complexes.

The future this monopoly portends is censorship of scientific freedom and the entrenchment of inequality. Access to the computational power that will decide "the next century of wealth and security"—new drug discovery, breakthrough molecular simulation of novel materials, financial market optimization, and the breaking of public-key cryptography (RSA, elliptic-curve cryptography, and the like) that underpins modern secure society—is now fully controlled by the private clouds of gatekeeping monopolists. They hold the power to vet **who** computes and **for what purpose**, and to block or censor any computation that conflicts with their interests or national strategy at any time.

World Quantum Computer (WQC) is an explicit rebellion against this privileged-class **quantum hegemony**—an open-source protocol that achieves the **democratization of computational resources** through cryptoeconomics.

### 1.2 Breaking Physical Limits: From One Giant Machine to a Planetary Nervous System

Centralized players are obsessed with manufacturing "a single giant machine" loaded with ever more physical qubits. Yet scaling superconducting circuits, ion traps, and similar hardware hits exponential physical limits—the memory wall and the hardware wall—in noise (decoherence) control and manufacturing cost.

The WQC protocol abandons the dogma of building one physically perfect computer. Instead, it takes the approach of **cryptographically connecting all existing computing devices on Earth**—commercial GPUs, SoCs with unified memory, surplus data-center capacity—and transforming them into **a single distributed nervous system**.

Throughout human history, only a tiny privileged class could own supercomputers or physical quantum machines. WQC makes the very concept of "owning a computer" obsolete. People around the world contribute hardware to the protocol and share one another's compute power; the participants of the network **become the computer itself**. That is WQC's ultimate vision.

> **"We are the Computer."**
> (We do not own the computer. We **are** the computer.)

# 2. Physical and Structural Challenges to Solve

Contemporary computing science and the ecosystem of distributed ledger technology (DLT) face three seemingly insurmountable barriers. WQC defines these not merely as technical hurdles but as **structural defeats** that block the expansion of human intelligence—and seeks to dismantle them.

## 2.1 Censorship of Abundance: Oligopoly of Access and the Privatization of Science

Physical quantum processing units (QPUs) operated by centralized firms such as IBM, Google, and Rigetti—or petascale simulation clouds owned by Big Tech with thousands of nodes—have become fully **closed gardens (censored spaces)**.

Access requires not only exorbitant usage fees but also passing the **purpose-of-use reviews** imposed by providers. This is serious censorship against the essence of scientific inquiry: **freedom and anonymity**.

For example, researchers affiliated with certain nations or regions, or DAOs (decentralized autonomous organizations) pursuing open-source development of alternative energy or new drugs that conflict with corporate interests, live under the constant risk of having access cut without notice. When the source of wealth and intelligence—computational resources—is controlled by corporate will, the result is structural **censorship of abundance** that slows scientific progress.

## 2.2 The Memory Wall: Exponential Explosion of the State Vector

The most classical yet destructive approach to simulating quantum computation on general-purpose hardware is **state vector simulation**. To track the full quantum superposition (all probability amplitudes) of $n$ qubits, this method must materialize $2^n$ complex numbers in memory.

Memory demand grows **exponentially** with qubit count.

| Qubits ($n$) | Required Memory | Hardware Limit |
|---|---|---|
| **30 Qubits** | ~16 GiB | Typical consumer PC ceiling |
| **40 Qubits** | ~16 TiB | High-end data-center server clusters |

| Qubits ($n$) | Required Memory | Hardware Limit |
|---|---|---|
| **50 Qubits** | ~16 PiB | Entire memory of world-class petascale supercomputers (beyond practical limits) |

Building a single colossal supercomputer that can fully hold a state vector beyond 50 qubits is **physically impossible** under modern semiconductor physics and cost-effectiveness (ROI). This is **the Memory Wall**. Approaches that confine resources to one chassis or a closed cluster linked by a single high-speed internal bus have already hit theoretical limits.

## 2.3 The Futility of PoW: A Paradigm Shift from Thermodynamic Waste to Useful Work (PoUW)

Since Bitcoin's birth in 2008, Proof of Work (PoW) has proven the most robust method for eliminating centralized intermediaries and achieving trustless consensus. From a thermodynamic perspective, however, conventional PoW carries a fatal flaw.

Mining farms worldwide consume gigawatts executing **mathematically meaningless brute-force computation**: repeatedly changing a nonce until a hash function output meets a difficulty target. The resulting hash is consumed only to finalize the next block—dumping enormous heat and carbon into the environment while contributing **not a single bit** to human knowledge or scientific progress.

What is needed now is a paradigm shift that converts this thermodynamic waste into **useful work**—binding the security cost of maintaining the network directly to the executable cost of computations that advance humanity's frontier: quantum chemistry, cryptography, machine learning, and beyond (**Proof of Useful Work: PoUW**).

# 3. Technical Breakthrough: Hyper-Distributed Tensor Contraction

WQC overcomes the physical limits of holding quantum state vectors beyond 50 qubits by transforming quantum circuits into **tensor network (TN) representations** and applying **deterministic dynamic slicing**. This chapter defines the mathematical foundation by which tens of thousands of distributed Worker Nodes cooperatively compute a single massive quantum circuit in a **trustless** environment.

## 3.1 Tensor Network Slicing and Dynamic Optimization of Bond Dimension

Universal quantum circuit simulation beyond 100 qubits—the target of this protocol—is impossible even with all storage on Earth under conventional state vector methods. WQC makes it feasible through dynamic tensor network slicing.

Large quantum circuits are modeled not as state vectors loaded wholesale into memory, but as **collections of tensors**—gates as matrices, quantum states as indexed legs (dimensions). Simulating the full circuit reduces to **contraction**: collapsing tensor indices one by one.

The WQC Orchestrator analyzes the topology of the submitted circuit graph and dynamically identifies cut lines (slice axes) where **bond dimension** is minimized.

By fixing a specific index $i$ (dimension $d$) and splitting the circuit, **slicing** decomposes one colossal task into $d$ mutually independent **slice tasks**.

$$T_{\text{global}} = \sum_{k=1}^{d} T_{\text{slice}}^{(k)}$$

The greatest advantage of this mathematical decomposition is that **Worker Nodes require no real-time communication (synchronization)**. Each slice computes in parallel independently, enabling planetary-scale asynchronous grid computing unaffected by network latency.

## 3.2 Deterministic Proof of Useful Work (D-PoUW)

WQC eliminates the power waste of nondeterministic hash brute force entirely. **The process of executing quantum simulation (tensor contraction) and cryptographically proving its validity** becomes the network's security anchor (PoUW).

Worker Node $n$ receives tasks not governed by luck but **deterministic** incentive rewards $R$ proportional to computational complexity and the cost of generating the zk-STARK proof $\pi$ that guarantees it. This reward model is strictly defined as:

$$R = \text{Gas}_{\text{quantum}}(C, \pi) \times \text{BaseFee}$$

Where:

- $R$: Total $WQC token reward received by the Worker Node.
- $\text{Gas}_{\text{quantum}}(C, \pi)$: Endogenous **quantum gas** consumption integrating memory and compute cost of contracting circuit $C$, plus algebraic cost (NTT, etc.) of generating zk-STARK proof $\pi$.
- $\text{BaseFee}$: Gas unit price dynamically set by network-wide supply–demand (algorithmic control).

ASIC resistance in the WQC network—preventing governance oligopoly by giant specialized miners—is permanently enforced not by artificial memory-hard functions but by two **endogenous hardware barriers**:

1. **Tensor Contraction Bottleneck (Tensor Access Phase)**:
   Contracting indices of huge tensors exhibits **low arithmetic intensity**—the ratio of random memory buffer access to FLOPs is extremely high. No matter how densely compute units are integrated, the **memory wall** makes memory bandwidth the bottleneck.
2. **Proof Generation Bottleneck (STARK Proving Phase)**:
   Encoding contraction validity as AIR (Algebraic Intermediate Representation) constraints, then running NTT (Number Theoretic Transform) and FRI polynomial interpolation via Plonky3 and similar stacks. This demands ultra-wideband memory space for permuting millions of elements at speed.

Mining ASICs optimized only for generic ALU density are completely disadvantaged in ROI versus manufacturing cost for terabyte-scale random access and wideband memory (HBM, etc.). Commercial high-end GPUs (NVIDIA RTX series, etc.) and consumer SoCs with wideband unified memory (Apple M series, etc.) therefore achieve the highest execution efficiency by design—**forcing hardware democratization**.

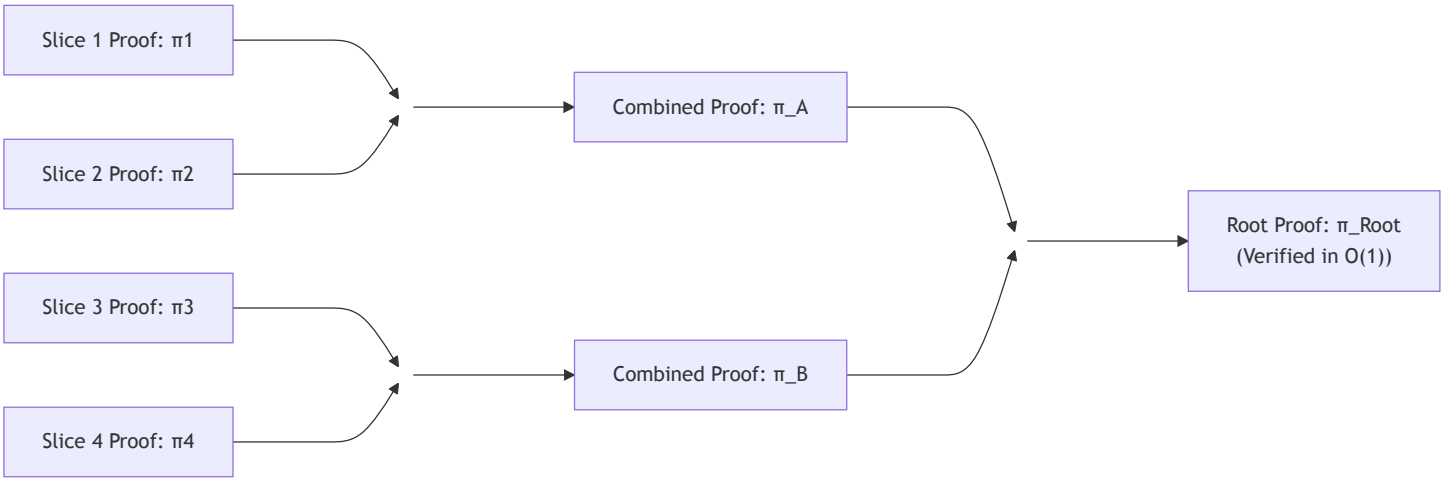
## 3.3 Deterministic Verification via zk-STARKs and Recursive Proof (Recursive Aggregation Pipeline)

Having the Orchestrator or Layer-2 smart contracts re-execute and verify each result from tens of thousands of nodes would instantly collapse the system. WQC resolves exploding verification cost through **recursive proof composition**.

Each Worker Node performs contraction on its assigned slice and simultaneously generates cryptographic proof $\pi_{\text{slice}}$ of mathematical validity. Binding the following **public inputs** into the STARK circuit prevents task substitution, wrong slice branches, data tampering, and theft (front-running) of other nodes' results:

$$\text{Public Inputs} = \{\text{circuit\_id},\ \text{sub\_task\_id},\ \text{node\_id},\ \text{slice\_id},\ \text{output\_result\_hash}\}$$

Rather than verifying every $\pi_{\text{slice}}$ directly, the Orchestrator (or aggregator) performs **recursive composition** in a tree (Proof Tree): generating **one new proof that verifies the fact that proofs $\pi_1$ and $\pi_2$ are both valid**.




Through this compression pipeline, the validity of thousands or tens of thousands of node computations converges to a single root proof ($\pi_{\text{Root}}$).

Aggregation is designed in stages: starting from native leaf-level STARK verification, progressing to binary tree combination via Aggregation STARK that binds child proof digests, and ultimately reaching full in-circuit recursion. Once complete, Layer-2 verifiers need verify only $\pi_{\text{Root}}$; verification cost is bounded at $\mathcal{O}(\log^2 M)$ in proof tree depth. Exploiting mathematical asymmetry—heavy generation, instant verification—WQC gains overwhelming scalability.

## 3.4 Execution Model: Practical Quantum Algorithms and Deterministic Sampling

The domain of useful work (PoUW) that WQC targets is not limited to computing a specific amplitude of a single quantum state vector. Applying practical algorithms such as VQE for molecular energy calculation, QAOA for combinatorial optimization, and dynamic circuits for quantum error correction to real-world problems requires an execution model that treats the resulting **measurement histograms** and **expectation values** as deterministic quantities free of probabilistic fluctuation.

Distributed networks, however, cannot satisfy this requirement straightforwardly. Even when different nodes compute the same circuit, a unified verification framework is needed to handle the probabilistic nature of quantum sampling, the

destruction of quantum correlations by measurement gates, and conditional branching within circuits. WQC resolves this challenge through the following four components.

### 3.4.1 Polymorphic Output Modes

What constitutes the result of a quantum circuit computation differs entirely depending on the algorithm's purpose. VQE requires the **expectation value of a Hamiltonian**, QAOA is decided by the **frequency of measured bit strings**, while for D-PoUW mining the minimum verification unit is a **single complex probability amplitude** at a specific register.

Rather than forcibly stuffing these into a single data format, WQC provides three output modes optimized for each use case.

- **Statevector Scalar Mode ( `statevector_scalar` )**: Pinpoint-contracts the complex probability amplitude corresponding to a specific register (e.g., $|0\rangle^{\otimes n}$). As the minimal unit for zk-STARK leaf proofs, it enables the lightest and fastest verification.
- **Measurement Sampling Mode ( `sample_counts` )**: Performs deterministic pseudorandom sampling for a specified number of trials ( `shots` ) on measurement gates, generating bit-string occurrence frequencies (histograms). By chaining the seed value, different nodes agree on an identical histogram.
- **Observable Expectation Mode ( `expectation` )**: For a Hamiltonian expressed as a linear combination of Pauli operators, algebraically computes the expectation value directly from the post-contraction state vector. Because this is not shot-based statistical estimation, consistent results are obtained across nodes even in a distributed environment.

### 3.4.2 Measurement-Preserving Policy (MP1 / OP1) for Multi-Slice Optimization

Tensor network slicing is a powerful technique for parallelizing computation. However, indiscriminately fixing the qubit axes targeted by measurement destroys the quantum-mechanical superposition (coherence) of the measurement results, preventing correct sampling or expectation values. To resolve this trade-off, WQC imposes constraints on slice axis selection per output mode.

- **Measurement-Preserving Policy (MP1)**: In sampling mode, qubit axes subject to terminal measurement ( `MEASURE` ) are automatically excluded from slice partitioning. Only non-measured qubits are compactly sliced, so contraction executes while preserving the measured quantum state in full, subject to Worker node memory constraints.
- **Observable-Preserving Policy (OP1)**: In expectation mode, fixing qubit axes on which the requested Pauli operators ($X$, $Y$, $Z$) act non-trivially is prohibited. This enables efficient parallel dispatch for circuits exceeding 28 qubits by extracting only the relevant qubit neighborhood.

### 3.4.3 Trajectory Separation for Dynamic Quantum Circuits (Mid-Circuit Measurement)

Quantum error correction and quantum walk simulation require **dynamic circuits** that perform mid-circuit measurement and conditionally branch subsequent gates based on the result. Such destructive measurements, however, cannot be handled by existing STARK proof frameworks that assume purely unitary operations without measurement.

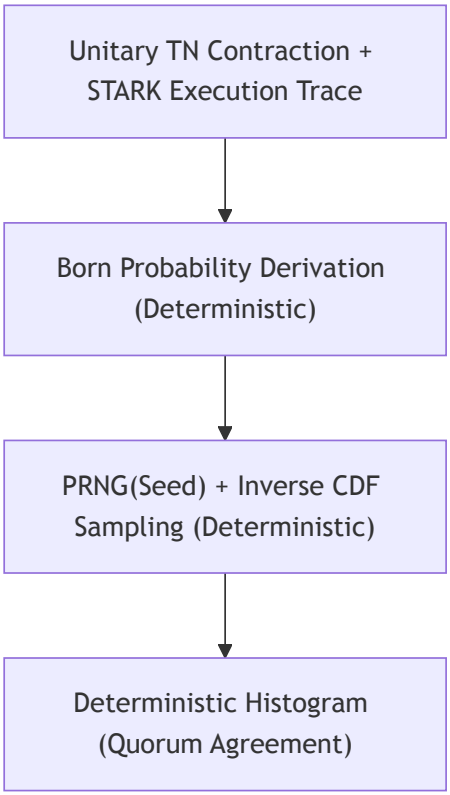
WQC solves this by fully separating **unitary traces** from **trajectory segments**. First, only the unitary portion with all destructive measurements removed is subjected to STARK proving. Then, the measurement events and classical register evolution occurring in each shot are independently bound as separate trajectory segments. By cryptographically chaining the state digest immediately before the first measurement ( `unitary_link_digest` ),

consistency between the unitary proof and trajectory segments is guaranteed. This successfully integrates the validity of complex dynamic circuits containing classical conditional branching into the proof tree.

### 3.4.4 PRNG Binding and Born Rule Zero-Knowledge Proof

The foundation of consensus lies in **deterministic verification**. Yet quantum-mechanical sampling is inherently probabilistic: if each node independently used physical randomness for measurement, even from an identical circuit and state, different nodes would generate different histograms. Quorum cannot be established under such conditions.

WQC resolves this dilemma of **deterministic consensus** and **probabilistic sampling** through a **deterministic resampling pipeline**.




The concrete flow is as follows. The Orchestrator distributes a unique seed value ( `sample_seed` ) to all Workers. Each Worker runs inverse cumulative distribution sampling using deterministic pseudorandom numbers seeded from this value over the exact probability distribution (Born probabilities) obtained from tensor contraction. All Workers thereby derive an identical histogram.

Furthermore, that the probability distribution was correctly derived from the quantum state vector is attested as a partial zero-knowledge proof using a dedicated STARK circuit ( `DistributionAir` ). The client can mathematically verify that the presented sampling results contain no probability fluctuation or tampering, but are a deterministic outcome derived purely from the laws of quantum mechanics and the designated seed.

# 4. Tokenomics & Governance

WQC's economic design is grounded in cryptoeconomics where token value is determined purely by the cycle of **computational resource provision and consumption**, completely excluding governance oligopoly by capital. To prevent rounding error and precision loss on computers, all currency and fee calculations in the protocol use 18-decimal fixed-point arithmetic (arbitrary-precision integers) without floating point.

### Currency Unit System

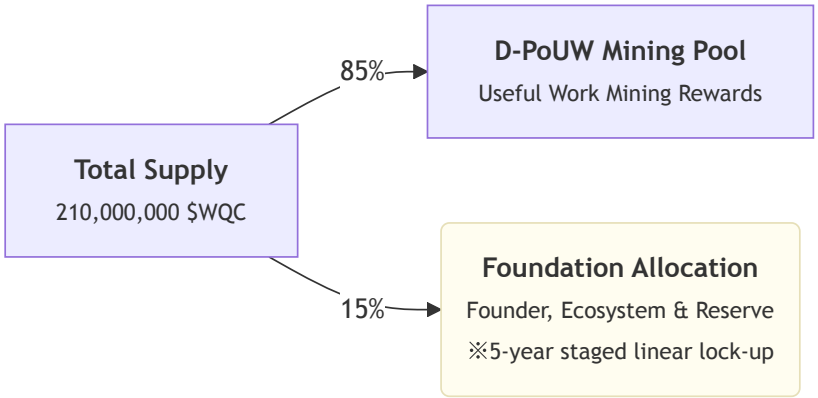
Currency and economic value in this protocol are strictly defined and managed by three units:

| Unit | Symbol | Fraction of 1 $WQC | Origin and Use |
|---|---|---|---|
| **WQC** | $WQC | $10^0$ (1) | Base currency unit. |
| **Shannon** | $sWQC | $10^{-9}$ (one billionth) | **Base unit for quantum gas (Gas Price).** (Named for Claude Shannon, father of information theory) |
| **Planck** | $pWQC | $10^{-18}$ (one quintillionth) | **Absolute smallest unit in the protocol.** All code operates on **integers** in Planck units. (Named for the Planck constant, physics' minimum length) |

## 4.1 Supply Curve and Fair Launch Incentive Design

Total $WQC supply is fixed at **210,000,000 $WQC** (integer form: $210,000,000 \times 10^{18}$ Planck) with **no additional issuance under any circumstances**. The protocol adopts a **Pure Fair Launch** with no pre-sale or VC pre-allocation.

To secure initial contributors and sustained ecosystem development, total supply is strictly allocated and locked by smart contract at the following ratios:




### 4.1.1 Foundation Allocation Liquidity Restrictions (Vesting Contract Specification)

15% of total supply (31,500,000 $WQC) is allocated to the **WQC Foundation** for sustained development funding and founder team incentives. To prevent sudden inflationary pressure on markets and align founder and community interests long-term, the following **linear vesting** is enforced by L2 smart contract:

- **Cliff**: For 12 months from network launch (Genesis), not a single Planck of foundation allocation may be withdrawn (fully locked).
- **Linear Release**: After cliff, liquidity unlocks evenly in Planck units over the remaining 48 months (5 years total), second-by-second (timestamp-dependent).

### 4.1.2 Founder Mining (The Early Adopter Advantage)

In the earliest period after Genesis when participation is lowest, it is fully legitimate on-protocol for the founding team to deploy compute resources (GPU/VRAM) and run D-PoUW—and it represents the greatest opportunity for **real yield**. Like Bitcoin, game-theoretic incentives ensure nodes that take early risk and support the network at peak efficiency earn the most $WQC (Planck); founders can build wealth openly and fairly.

## 4.2 Quantum Gas Market Price Mechanism

When clients request quantum circuit simulation, fees consumed are computed as **quantum gas**. Required gas for one task is:

$$\mathrm{Gas}_{\mathrm{quantum}}(C, \pi) = \alpha \cdot \mathrm{VRAM}_{\mathrm{peak}}(C) + \beta \cdot \mathrm{FLOPs}(C) + \gamma \cdot \mathrm{ProvingTime}(\pi) + \delta \cdot \mathrm{SampleCost}(C, \mathrm{shots})$$

Here $\mathrm{SampleCost}$ is a cost term for measurement post-processing and histogram aggregation when `output_mode` is `sample_counts` or `expectation`. For `statevector_scalar` only tasks, $\delta = 0$.

The transaction fee clients actually pay ($\mathrm{Total\ Fee}$) multiplies this gas by dynamically varying gas unit price $\mathrm{BaseFee}$ (unit: Shannon / Gas) according to network congestion:

$$\mathrm{Total\ Fee\ (in\ Planck)} = \mathrm{Gas}_{\mathrm{quantum}}(C, \pi) \times \mathrm{BaseFee} \times 10^9$$

When the global pending task queue exceeds a threshold, $\mathrm{BaseFee}$ rises automatically to encourage node entry (supply increase). When demand falls, $\mathrm{BaseFee}$ converges to a floor, offering clients low-cost computation. All multiplication and addition in orchestrator internals and on-chain use arbitrary-precision integers (Go `big.Int`, Rust `U256`, etc.)—**not a single Planck of rounding error**.

## 4.3 20% Automatic Burn (Deflationary Burn) and Economic Sustainability

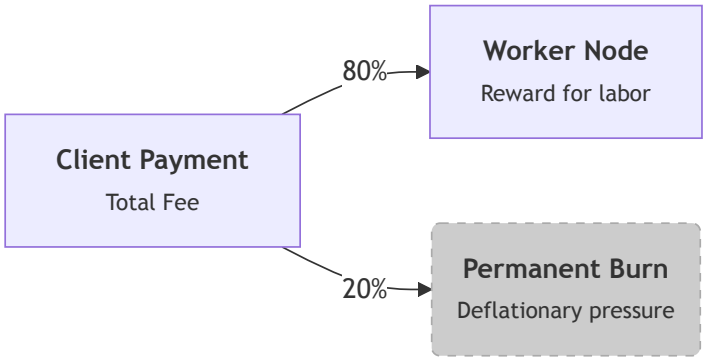
To provide permanent deflationary pressure (upward price pressure) on the WQC ecosystem, **20% of total fees (** $\mathrm{Total\ Fee}$**) paid by clients is immediately sent to a burn address by smart contract at settlement and permanently destroyed (burned)**.

Net reward $R_{\mathrm{net}}$ received by Worker Node $n$ is enforced by integer arithmetic:

$$R_{\mathrm{net}} = \lfloor \mathrm{Total\ Fee} \times 80 \div 100 \rfloor$$

$$\mathrm{Burn\ Amount} = \mathrm{Total\ Fee} - R_{\mathrm{net}}$$

(Here $\lfloor \dots \rfloor$ denotes integer division truncating remainder. Sub-Planck remainder from truncation is added to Burn Amount automatically.)




### 4.3.1 Mathematical Consequences of Deflationary Economics

With this 20% automatic burn, the higher WQC usage (compute demand), the faster circulating $WQC supply decreases.

$$\frac{d(\text{Supply})}{dt} = -0.20 \times \sum_i \text{Total Fee}_i$$

In this absolute deflation model, even if total supply shrinks and per-$WQC market value soars extremely, the protocol supports payments subdivided to 18 decimal places (Planck units), so **settlement gridlock (liquidity crisis) cannot occur in principle**.

In a future of soaring value, setting $\text{BaseFee}$ as low as `1 Planck` level lets clients always request quantum computation at fair, tiny costs aligned with real fiat rates, while all token holders (founders, miners, long-term investors) enjoy sustained asset appreciation—a mathematically guaranteed **flywheel**.

# 5. Development Roadmap: Path to the Sovereign Network

WQC evolves from single-machine verification through public testnet validation to a mainnet release with on-chain settlement, and ultimately to a **fully autonomous quantum compute network (Sovereign Network)** censored by no nation or corporation.

## 5.1 Phase 1: Foundation — Complete

Establishing single-node simulation engine and minimal end-to-end protocol pipeline proof.

- **Universal Gate Set**: `wqc-core` (Rust) supports major quantum gates (H, X, Y, Z, T, CNOT, CCNOT, etc.), enabling up to ~30-qubit state vector simulation on consumer hardware.
- **End-to-End Vertical Slice**: Connected Orchestrator, Worker Node, and Core; demonstrated pipeline from client submission through node compute to result aggregation.
- **Deterministic PoUW Prototype**: Abolished meaningless hash mining; confirmed "quantum circuit simulation + zk-STARK proof generation" operates as designed in a closed environment.

## 5.2 Phase 2: Scaling & Swarm Distribution — In Development

Building the skeleton of a planetary Swarm on **libp2p**, connecting bidding, slice partitioning, verification, and off-chain economics.

### 5.2.1 devnet PoC Status

The following core modules have passed end-to-end (e2e) verification in the current development environment (devnet):

- **libp2p Swarm Communication**: P2P implementation of task announcement via Gossip protocol, bid stream, dispatch, and result return.
- **Permissionless Bidding and Quorum**: Signed bidding, weighted lottery selection, node capability matching, slice-level majority vote (floating-point epsilon agreement and counts exact match).
- **Dynamic Slice Partitioning (Policy C)**: BFS slice tree generation based on bid pool max-qubit capability, and establishment of an asynchronous execution model.
- **Automated Proof Aggregation (R1+R2)**: From leaf STARK verification to single root-verification STARK via Aggregation STARK constructing a binary tree.
- **Polymorphic Output Modes and Born Rule Proof (Phase A–C)**: Sampling ( `sample_counts` ) and expectation ( `expectation` ) modes, dynamic circuits (Mid-Circuit MEASURE), deterministic resampling via seed binding, and `DistributionAir` implementation for probability distribution validity.

### 5.2.2 Public Testnet

As the culmination of Phase 2, a **Public Testnet**—an open verification environment—will be released prior to mainnet launch. This testnet maintains Swarm logic equivalent to mainnet while prioritizing operational stability and efficient early debugging under the following specifications:

- **Open-Source Repositories and Permissionless Participation**: All relevant source code will be made fully public. Anyone worldwide can download a Worker node client, contribute their local compute resources (GPU/VRAM), and participate in verification on a trial basis.
- **Centralized Orchestrator Operation**: To guarantee task coordination and infrastructure stability, a single Orchestrator managed by the protocol foundation will operate during this phase.
- **Redis-Based Test Economy and Faucet**: The economic zone and settlement log adopt the Redis-based high-speed off-chain architecture carried over from devnet. A **Faucet** web interface will provide anyone with free test $WQC tokens, enabling stress-testing of the incentive design (E1–E4) under real traffic.
- **No Physical QPU Proxy**: At this stage, no physical QPU connection will be made; verification focuses purely on classical distributed simulation.

## 5.3 Phase 3: Mainnet Launch & On-chain Settlement — Next Target

Following sufficient operational track record and security audits on the Public Testnet, the protocol transitions to the production environment (Mainnet), achieving full societal implementation of the tokenomics.

- **Full On-chain Settlement (E5)**: End the provisional Redis-based operation of the testnet; deploy a complete on-chain settlement infrastructure on L2 smart contracts. On-chain verification of root proof $\pi_{\mathrm{Root}}$, distribution of genuine $WQC tokens with real value to Workers, and 20% automatic burn are all executed under the absolute sovereignty of code. The Foundation's 5-year linear lock-up (vesting) contract is also activated on-chain.

- **Stable Operation Beyond 50 Qubits**: Optimize the Swarm power of globally distributed wideband nodes to stably accept and process universal quantum circuit simulations exceeding 50 qubits—beyond the limits of a single superclass supercomputer—as commercial and scientific tasks.

## 5.4 Post-Mainnet Evolution: Full Sovereignty and Hardware Integration

After mainnet launch, once 50-qubit-class simulation is established as distributed infrastructure and the network achieves economic and technical stability, the following long-term expansion roadmap will be initiated.

- **DHT-Based Orchestrator Full Decentralization**: Eliminate dependence on a single Orchestrator (a centralized single point of failure and censorship risk). Transition to an architecture where multiple aggregators coordinate autonomously via DHT over P2P for task partitioning, assignment, and aggregation, completing a true **Sovereign Network**.
- **Physical QPU Proxy Integration**: Go beyond a network of classical simulator nodes; enable external independent physical quantum computers (QPUs) to be plugged in as Workers via a standard interface. This elevates WQC from a "planetary-scale distributed classical simulator" to an **ultimate distributed quantum computing fabric fusing real machines with simulators**.

# 6. Conclusion: We are the Computer.

The World Quantum Computer (WQC) protocol does not aim merely to replace existing supercomputers or quantum computers. It is a **cryptoeconomic paradigm shift** to destroy the monopoly structure of computational resources distorted by wealth and power—and return the freedom of scientific inquiry to everyone's hands.

Humanity has long paid the price of **convenience** from technological progress with dependence on giant platform gatekeepers and the censorship that follows. That even "next-generation compute power" essential to new drug development, understanding the cosmos, and designing cryptography that secures society is being privatized by a small privileged class is the greatest bottleneck to the evolution of human intelligence.

WQC rebels against this centralized hegemony with the force of mathematics and economic rationality.

1. **Overcoming Physical Limits**:
   Abandon the dogma of building one colossal machine; unify Earth's dormant devices into one nervous system through tensor network slicing.
2. **Practical Quantum Execution Model**:
   Go beyond single-amplitude computation; natively support measurement, sampling ( `MEASURE` / `shots` / `counts` ), and Pauli expectation values as first-class outputs. Guarantee the cryptographic validity of sampling results in a distributed environment via deterministic PRNG binding and Born rule zero-knowledge proofs.
3. **End of Wasted Energy**:
   End the era of nondeterministic hash mining that erodes the planet; convert cryptographic zk-STARK proof generation itself into **Deterministic Proof of Useful Work (D-PoUW)**.
4. **Embodiment of Complete Fairness**:
   Enforce by code a Pure Fair Launch with no pre-sale or VC allocation; distribute sovereignty and rewards only to pure contributors to the network.

WQC is neither a "product" owned by some corporation nor "infrastructure" managed by a particular state. It is humanity's first **open-source intelligence at planetary scale with no centralized master**.

The era of paying high fees to "own" computers from the outside is over. People worldwide connect their hardware to the protocol, share compute power, and drive the network autonomously. At that moment, the participants of the network themselves become the world's largest computer.

> **"We are the Computer."**
> (We do not own the computer. We **are** the computer.)