Freedom from unwanted hacking through Distributed Ledger Technology on the World's First Quantum-Resistant Blockchain!

Quantarium

ENGLISH
White paper v2.1

Steve Jung
Co-Founder, CEO

Quantarium Coin White Paper

CONTENTS

1. Executive Summary

1.1 Project Overview: The Necessity of Native Quantum-Resistant Blockchain

Cryptographic Trust, the foundation of the digital economy, is currently facing a critical turning point. The RSA and Elliptic Curve Cryptography (ECC/ECDSA) systems, which have supported the internet and blockchain industries for decades, are on the verge of having their computational complexity assumptions(specifically the integer factorization and discrete logarithm problems)collapsed due to the rapid advancement of Quantum Computing.

The practical implementation of Logical Qubits and the development of hybrid quantum algorithms are accelerating the arrival of 'Quantum Supremacy.' This poses an existential threat to all blockchain networks that rely on existing Public Key Infrastructure (PKI).

In particular, the 'Harvest Now, Decrypt Later (HNDL)' attack scenario, where attackers collect encrypted data now to decrypt it with future quantum computers, is an urgent security issue of the present, not the future.

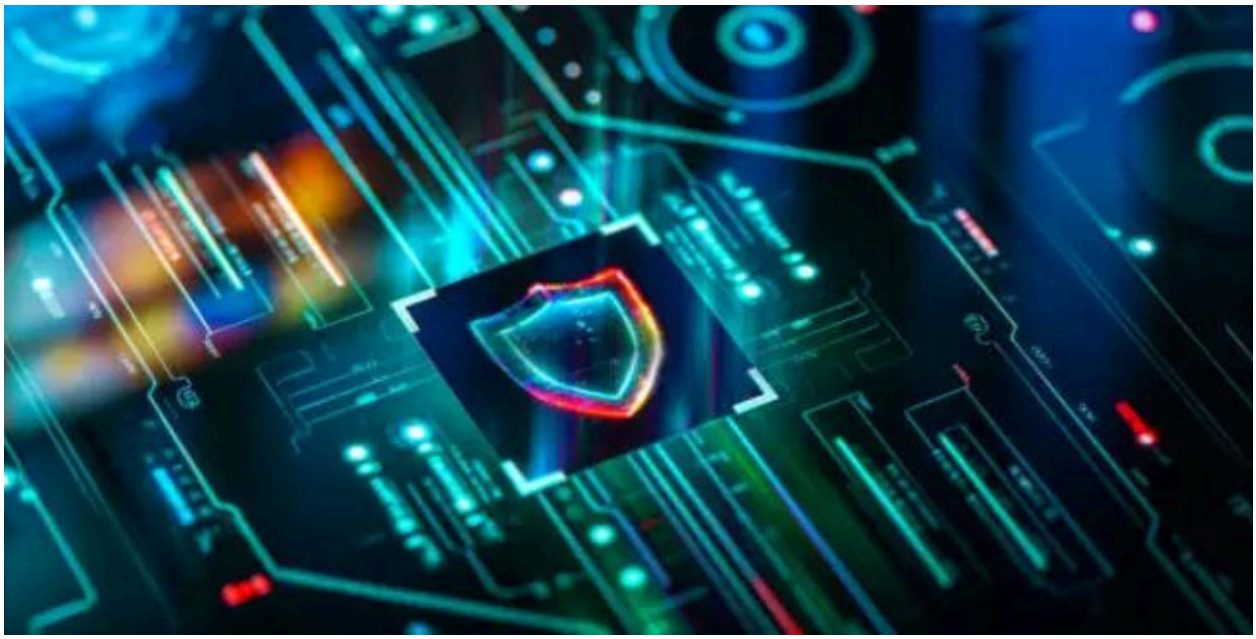
Most existing blockchains (Bitcoin, Ethereum, etc.) were designed without considering Post-Quantum Cryptography (PQC). Even if they upgrade to PQC signatures via soft forks in the future, all transaction records generated from the Genesis Block up to the point of the upgrade will remain under the vulnerable legacy encryption scheme. We define this as 'Quantum Legacy Vulnerability,' which undermines the intrinsic value of blockchain: guaranteeing the permanent ownership of assets.

Quantarium was born to solve this structural dilemma. Quantarium rejects the post-hoc approach of adding quantum resistance to existing systems. Instead, it is a '**Native Quantum-Resistant Layer 1 Blockchain**' that applies post-quantum cryptographic algorithms to every transaction, signature, and verification process starting from the very first block, the **Genesis Block**. Quantarium presents a standard for next-generation digital trust infrastructure that guarantees data integrity and asset safety that remains immutable even in the quantum era.

1.2 Core Value Proposition

Quantarium is not merely a technical experiment; it is a practical blockchain solution that meets enterprise and public infrastructure-level requirements. Our core values are defined by the following four pillars

- **Standard Compliance :** Quantarium does not use proprietary or unverified cryptographic algorithms. We have adopted the **SPHINCS+** family of algorithms, which was finally selected as the Post-Quantum Cryptography digital signature standard (FIPS 205) by the National Institute of Standards and Technology (NIST), as our core security engine **(QUANTA-X)**. SPHINCS+ uses a purely hash-based signature method that does not rely on mathematical hard problems, providing the most conservative and certain security that will not collapse even if unknown mathematical attack techniques are discovered.
- **Legacy-Free Integrity :** The 'Native Layer 1' structure, with PQC applied from the design phase, fundamentally blocks retroactive hacking threats against past data. This provides the only solution for fields requiring ultra-long-term trust, such as financial assets requiring long-term value preservation, Real World Asset (RWA) tokenization, and national archives management.
- **High Performance & Consensus :** Security must not mean a degradation in performance. Quantarium has adopted the Proof of Authority (PoA) consensus mechanism to eliminate unnecessary mining competition. By ensuring high throughput and instant finality through identity-verified nodes (Validators), we have built a commercial environment capable of real-time payments and large-scale transaction processing.
- **Unified Security Ecosystem :** Quantarium provides a 'Quantum-Resilient Security Loop' that extends beyond the blockchain network. We apply the same PQC security stack to the entire process—from user private key generation and asset transfer (Wallet), to network consensus (Consensus), and data communication (SECURET Messenger)—providing a complete security environment that eliminates Single Points of Failure within the system.



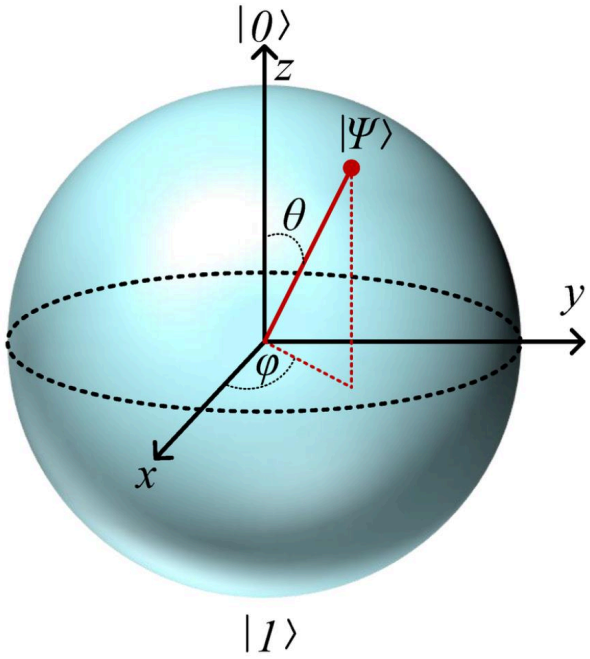
2. Market Context & Threat Model

2.1 Advancement of Quantum Computing & The Cryptographic Crisis

Modern Information Technology (IT) infrastructure relies on cryptographic systems designed within the limits of classical computers that perform bit-based (0 and 1) operations. However, the rapid advancement of **Quantum Computing** technology, which utilizes the principles of quantum mechanics such as **Superposition** and **Entanglement**, is fundamentally shaking these premises.

Recently, major technology companies such as IBM, Google, and Quantinuum have moved beyond processors with hundreds of qubits to the stage of '**Logical Qubits**' capable of Error Correction. This indicates that quantum computers are moving out of the laboratory and entering a commercialization phase with substantial computational capabilities.

From a cryptographic perspective, this progress is defined as a 'crisis.' The security of modern Public Key Infrastructure (PKI) is based on the **Computational Complexity** assumption that solving 'integer factorization of large numbers' or 'discrete logarithm problems' takes an astronomical amount of time. However, a quantum computer equipped with **Shor's Algorithm** can solve these mathematical hard problems within **Polynomial Time**, possessing the potential to break the dam of security that upholds existing internet communications and financial transactions.



Visualization of the state of a qubit Ψ in the Bloch sphere

2.2 Structural Collapse Risk of Legacy Blockchains based on RSA/ECC

The core of blockchain technology is decentralized trust, which is guaranteed through **Digital Signatures.** The majority of major blockchain networks existing today, including Bitcoin and Ethereum, use Elliptic Curve Cryptography (ECC), specifically the **ECDSA (Elliptic Curve Digital Signature Algorithm)** or RSA algorithms.

If the era of Quantum Supremacy arrives, these legacy blockchains face the following structural collapse risks

1. **Public Key Reversal & Wallet Theft** : Using Shor's Algorithm, a private key can be derived from a public key exposed on the blockchain. This means an attacker can transfer assets or hijack smart contract permissions without the legitimate owner's knowledge.
2. **Transaction Forgery :** If the Elliptic Curve Discrete Logarithm Problem (ECDLP) is neutralized, attackers can forge valid digital signatures. This destroys the Integrity of the blockchain and enables Double Spending attacks, potentially causing the economic value of the network to converge to zero.
3. **Consensus Algorithm Paralysis :** Validator signatures are essential even in consensus processes like PoS (Proof of Stake). If the signature scheme is breached, the consensus of the entire network can be manipulated or paralyzed.
4. **Weakening of Hash Algorithms via Grover's Algorithm** While Shor's Algorithm neutralizes asymmetric key cryptography (digital signatures), Grover's Algorithm threatens the Hash Functions that guarantee the blockchain's connection structure and integrity.
    - **Quantum Acceleration and Halving of Security Level** : Grover's algorithm provides a quantum acceleration (Quadratic Speedup) for unstructured data search, weakening the Collision Resistance of hash functions. Theoretically, this has the effect of reducing the security strength of currently used hash algorithms like SHA-256 to half (128-bit).
    - **Difference in Countermeasures :** For hash functions, defense against quantum threats is partially possible by increasing the output length (e.g., SHA-256 → SHA-512). However, since the mathematical hardness of digital signatures (ECDSA) itself is collapsed by Shor's algorithm, defense via simple key length extension is impossible, and a full algorithmic replacement with Post-Quantum Cryptography (PQC) is the only solution.
5. **Conclusion: Inevitability of Structural Transition** Consequently, existing blockchains face an 'Existential Threat' in the areas of wallet security and digital signatures that prove ownership. Therefore, for sustainable blockchain security, a structural transition to an infrastructure equipped with PQC digital signatures from the design phase is essential, rather than a gradual modification of the existing system.

2.3 'Harvest Now, Decrypt Later' Attack & Legacy Vulnerability

Security threats exist even now, before the commercialization of quantum computers, due to the **'Harvest Now, Decrypt Later (HNDL)'** attack scenario.

1. **Attack Mechanism :** Hackers or hostile state agencies collect and store data protected by current encryption technologies (transaction records, communication packets, etc.) in bulk, even if they cannot decrypt it now. They will then decrypt it en masse when a quantum computer with sufficient performance is developed in the future.
2. **The Blockchain Immutability Paradox :** Blockchain's 'immutability' becomes a fatal weakness in this attack scenario. Data once recorded on the blockchain cannot be deleted or modified. Therefore, transaction records currently generated based on RSA/ECC are destined to be permanently exposed in the future.
3. **Legacy Vulnerability :** Even if existing blockchains upgrade to PQC via a soft fork in the future, past addresses and transactions generated before the upgrade remain signed with the old algorithm. Attackers can use this past data to secure an Entry Point or steal assets that have not moved for a long time (Sleeper Wallets). We call this **'Quantum Legacy Vulnerability'** a fundamental problem that cannot be solved by retroactive measures.

2.4 Urgency of PQC Transition & Global Standardization

Global standardization efforts to counter quantum threats have already moved beyond the 'preparation' phase into the 'implementation' phase.

- **NIST Standardization Complete :** Through a PQC competition conducted since 2016, the U.S. National Institute of Standards and Technology (NIST) officially announced SPHINCS+ (SLH-DSA), Kyber (ML-KEM), and Dilithium (ML-DSA) as final standard algorithms (FIPS) in August 2024. This confirms that PQC is no longer an experimental technology but an industrial standard.
- **Government Mandates :** The U.S. White House, through National Security Memorandum (NSM-10), has directed all federal agencies to transition their systems to PQC by 2035, and the NSA is also encouraging the transition by releasing the CNSA 2.0 suite.
- **Urgency :** System migration typically takes years. Considering that the speed of quantum computer development may be faster than expected (the Y2Q problem), systems that do not adopt PQC immediately will reach a state of 'Security Bankruptcy,' not just future Technical Debt.

Therefore, the emergence of Quantarium, equipped with the NIST standard SPHINCS+, is not just technical progress, but the only urgent alternative that meets the changing global security standards.

3. Solution & Philosophy

Quantarium is not an **Incremental Improvement** to overcome the limitations of existing blockchains, but a **Fundamental Redesign** to respond to the paradigm shift of the quantum computing era. Our solution sets security as a non-negotiable top priority and is designed based on two core pillars : **Native PQC** and **NIST Standard Compliance.**

3.1 Design Principles: Security-First & Immutability

Quantarium's architecture follows the '**Security-First**' principle at every design stage. This means we do not sacrifice security for Scalability or Usability.

- **Definition of True Immutability :** The immutability claimed by existing blockchains assumes 'current computing power.' However, true immutability means data must remain unchanged and protected even against the computational power of quantum computers. Quantarium is designed to satisfy the proposition that "data recorded today cannot be forged or altered by any future technical advancement."
- **Zero Trust Based Design :** We do not trust future computing environments, let alone network participants. Therefore, we assume the potential development of decryption technologies and minimize risk by applying only the most conservative and verified cryptographic methodologies.
- **Long-term Data Survivability :** Financial assets, identity information, and public records must be preserved for decades. Quantarium aims for '**Digital Permanence**' guaranteeing data integrity 50 or 100 years from now, rather than competing for short-term transaction processing speeds.

3.2 Native Post-Quantum Cryptography Architecture

Many blockchain projects plan hybrid approaches adding PQC on top of existing algorithms (RSA/ECC) or migrations via soft forks. However, Quantarium takes a '**Native**' approach where PQC is applied from the **Genesis Block.**

- **Zero Legacy :** Upgrade methods for existing chains leave a 'Legacy Vulnerability' where past data (Old Tx) prior to the upgrade remains under the old encryption scheme. Because Quantarium applies quantum-resistant algorithms from the starting point, there are no **Weak Links** vulnerable to quantum attacks in the entire history of the network.

- **Full-Stack Security :** Quantum resistance is not limited to a specific layer.
    1. **Wallet Layer :** PQC application from address generation and key management.
    2. **Transaction Layer :** Asset transfer signing and verification.
    3. **Consensus Layer :** Consensus messages between validator nodes and block proposal signatures.
- **Harvest Now, Decrypt Later Defense :** The Native PQC architecture makes even currently collected encrypted data packets indecipherable by quantum computers. This perfectly extends data confidentiality and integrity into the future.

3.3 NIST Standard Compliance & Structural Resilience

Proprietary cryptographic algorithms risk containing unverified vulnerabilities. Quantarium has secured enterprise-grade reliability by complying with global security standards.

- **Adoption of NIST Standard SPHINCS+ :** We have adopted the **SPHINCS+** family, selected by the U.S. National Institute of Standards and Technology (NIST) as the standard for post-quantum digital signatures, as our core engine. This is an algorithm that has passed years of Public Review by the global cryptographic community, proving its mathematical safety.
- **Structural Resilience of Hash-Based Signatures :** Unlike Lattice-based cryptography, SPHINCS+ does not rely on specific mathematical structures (like SVP) but relies solely on the security of **Cryptographic Hash Functions.** This means that even if a new mathematical breakthrough threatens other PQC algorithms in the future, the system will not collapse as long as the hash function remains secure. Quantarium provides security like a last bastion through this **'Structural Resilience'**.
- **Regulatory Compatibility :** The adoption of NIST standards proactively meets security guidelines (e.g., CNSA 2.0) that governments and financial regulators will likely mandate in the future. This provides a decisive competitive advantage for Quantarium's adoption as institutional finance and public infrastructure.

4. QUANTA-X: Core Quantum-Resistant Crypto Engine

Quantarium has built a comprehensive 'PQC Security Stack' that encompasses the entire system, going beyond the application of a single cryptographic algorithm. This stack centers on the proprietary QUANTA-X engine, combining the integrity of the NIST standard algorithm SPHINCS+ with the stability of a Stateless architecture to complete an enterprise-grade blockchain infrastructure.

4.1 QUANTA-X Engine: The Core of Next-Gen Security

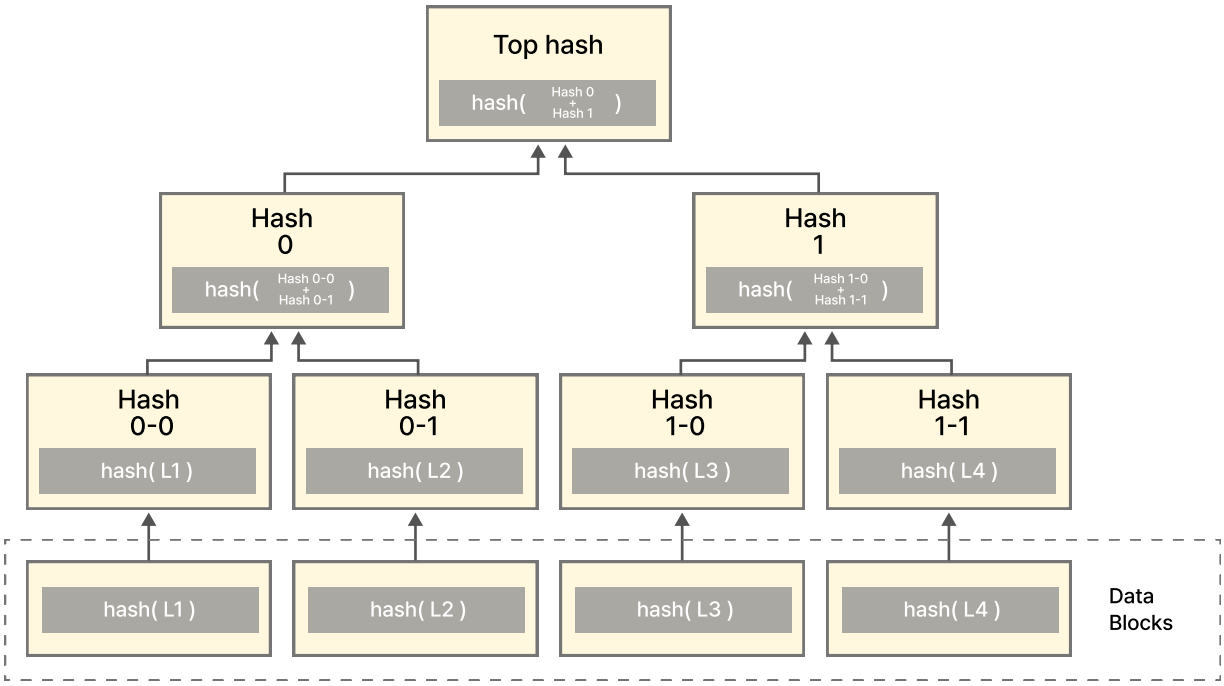
QUANTA-X is a high-performance security engine dedicated to cryptographic operations on the Quantarium network. It is not just an algorithm library but an integrated cryptographic module optimized for the blockchain environment, performing the following core functions :

- **Hybrid Key Management System (KMS) :** Processes the generation, storage, and loading of PQC Key Pairs in an isolated memory space to defend against Side-Channel Attacks
- **Signature Acceleration :** Includes acceleration logic that optimizes the relatively large signature size and verification time—characteristics of hash-based signatures—to meet blockchain real-time processing requirements (Latency).
- **Abstraction Layer :** Features a Modular structure that allows for flexible replacement and updates at the engine level without a hard fork, even if cryptographic standards change or new algorithms (e.g., NIST Round 4 candidates) emerge in the future.

4.2 QUANTA-X Algorithm: Pure Hash-Based Digital Signature

Quantarium has adopted **SPHINCS+ (SLH-DSA)**, established as the FIPS 205 standard by NIST, as the mainnet's default signing algorithm. This is the most conservative and safe choice that does not rely on mathematical hard problems, unlike Lattice-based cryptography.

- **Minimal Security Assumptions :** The security of SPHINCS+ relies solely on the **'security of cryptographic hash functions (collision resistance and preimage resistance).'** This means that even if methods to break integer factorization, discrete logarithm problems, or even lattice problems are discovered in the future, the system remains impenetrable as long as the hash function (SHA-256/SHAKE) is secure.
- **Long-Term Reliability :** Because it does not use specific mathematical structures, it is evaluated as the lowest-risk 'Fail-Safe' solution in a situation where the prediction of quantum algorithm development is uncertain.
- **Verified Standard :** By using an algorithm confirmed as a NIST standard through years of Public Review by cryptographers worldwide, we have fundamentally eliminated the possibility of backdoors or design errors that proprietary algorithms might have.



A structure where data blocks are connected in a tree-like form and converge to the top-level root hash

4.3 Stability via Stateless Architecture

Early hash-based signatures (XMSS, LMS, etc.) were **Stateful** methods that had to record the number of key usages. This had a fatal flaw where security would completely collapse if the same One-Time Signature (OTS) Key was reused due to a 'state synchronization' failure. Quantarium has perfectly solved this using the **Stateless** nature of SPHINCS+.

- **Multi-Signature & Backup Safety :** Even if a user restores a wallet from a backup or clones a Virtual Machine (VM) in a cloud environment, there is no need to manage a 'signature count.' This removes the complexity of node operation and prevents user errors.
- **FORS & WOTS+ Structure :** SPHINCS+ uses a Forest structure of random hash trees to probabilistically prevent key reuse without remembering state. This provides essential **'Asynchronous Security'** in a Distributed Ledger environment.
- **Integrity Assurance :** Even if billions of transactions occur, the security strength of the signing key does not degrade, technically supporting the non-stop operation of the blockchain.

5. Quantarium PQC Security Stack

NIST SPHINCS+ Implementation & Cryptographic Integrity

Quantarium's security stack is a collection of pure cryptographic engines and protocols operating within the network architecture. Beyond simply adopting the NIST standard SPHINCS+, we have applied proprietary implementation technologies that optimize it for blockchain constraints (storage space, computation speed) and maximize the safety of key management.

5.1 SPHINCS+: Structural Resilience via Hash-Based Signature

Quantarium has adopted **SPHINCS+**, which is designed to provide long-term cryptographic safety even in a quantum computer environment, unlike Lattice-based cryptography.

- **Independence from Mathematical Hard Problems :** SPHINCS+ is a purely **Hash-Based Post-Quantum** digital signature method that does not rely on integer factorization or discrete logarithm problems, which existing public key cryptography (RSA, ECC) depends on.
- **Structural Resilience :** Because it relies solely on the security of cryptographic hash functions, the security of the entire system does not collapse even if specific mathematical **Assumptions** crumble. This provides fundamental resilience allowing the Quantarium network to survive amidst uncertain changes in the future cryptographic environment.

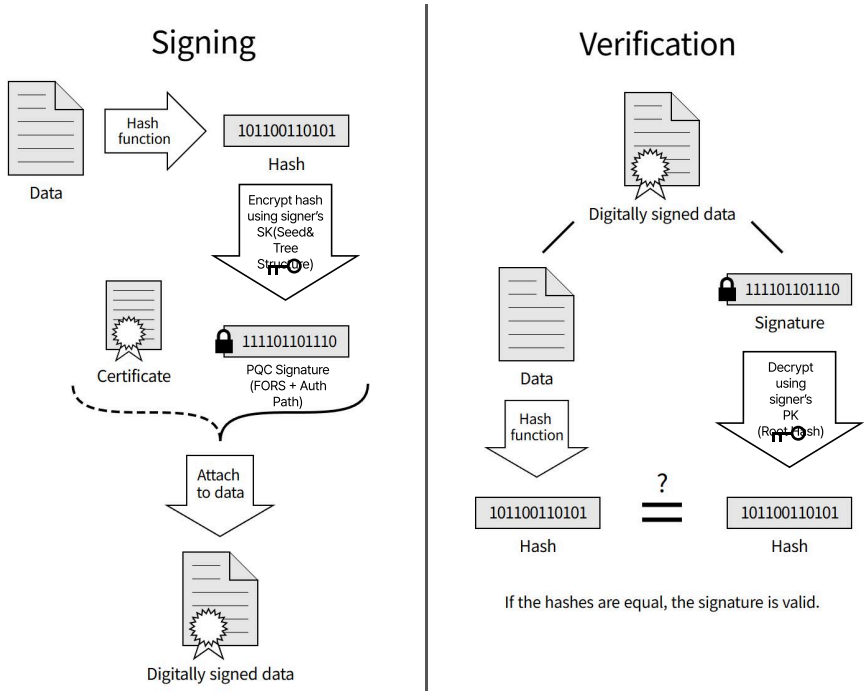


Diagram of Signing and Verification process using Hash, Private Key, Certificate, and Public Key

5.2 Core Application of PQC Mechanism

Quantarium has adopted the SPHINCS+ family structure not as an optional feature, but as the default digital signature mechanism controlling the entire network. This security stack is mandatorily used for the following core network activities :

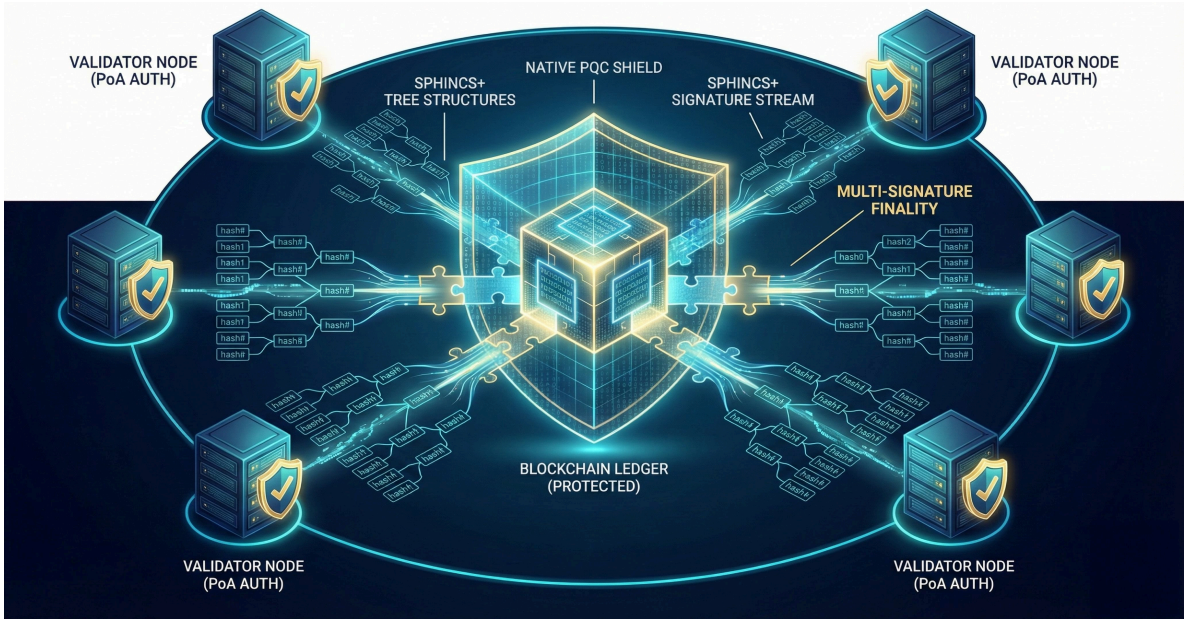
1. **Transaction Integrity :** Protects user private keys and proves transaction integrity during asset transfers and smart contract calls.
2. **Validator Authentication & Authority Proof :** Authenticates the legitimacy of nodes participating in PoA consensus with quantum-resistant cryptography, fundamentally blocking attacks on network governance.
3. **Cryptographic Proof in Consensus :** Protects all signing activities occurring throughout the network participation and consensus process, including block proposal, validation, and finalization.

5.3 Layered Integration & Domain Definition

Quantarium's PQC Security Stack is consistently applied across the Wallet layer, Sign/Verify layer, **Consensus Auth** layer, and **Messaging & Identity** layer, rather than remaining at a single point.

In particular, this security stack serves as a reference point that clearly separates the **Cryptographic Protection Domain** and the **Application Logic Domain** within the system architecture.

- **Transparent Definition of Responsibility :** By isolating the security stack to handle core cryptographic operations and the application logic to handle only business processes, the scope of security and limits of responsibility are transparently defined. This acts as a safeguard preventing errors in complex dApp logic from shaking the security foundation of the mainnet.



6. Layer 1 Architecture & Proof of Authority (PoA) Consensus

High-Performance PQC Consensus Model

Quantarium is an **Independent Layer 1 Blockchain** with its own protocol and ledger, not a token or sidechain dependent on another blockchain. We have adopted the **Proof of Authority (PoA)** consensus method to guarantee fast transaction processing and predictable network performance capable of enterprise-grade service, while absorbing the data overhead inevitably accompanied by Post-Quantum Cryptography (PQC) at the system level.

6.1 Purpose of Independent Layer 1 Infrastructure

While existing EVM-based Layer 2 solutions might solve scalability issues, they inevitably inherit the quantum vulnerability (ECDSA dependence) of the Base Layer, such as Ethereum.

- **Native Optimization :** Through an independent Layer 1 design, Quantarium has independently implemented a dedicated block structure and **Gas** policy capable of efficiently processing large signature data like SPHINCS+.
- **Sovereign Governance :** We have secured technical sovereignty to respond immediately to cryptographic issues, such as changes in NIST standards, without being swayed by hard forks or policy changes of external mainnets.

6.2 Operational Mechanics of PoA Consensus

Quantarium's PoA is a structure where a small number of verified nodes cooperate, rather than an anonymous majority competing.

- **No Mining Competition :** Unlike PoW (Proof of Work), we have completely eliminated meaningless hash computation competition. This reduces energy consumption by over 99% and focuses hardware resources solely on transaction verification and smart contract execution.
- **Low Latency & High Throughput :** We have minimized block propagation time by forming optimized P2P communication paths between a limited number of Validator Nodes. This enables stable high throughput of thousands of TPS or more and allows for real-time payment processing without bottlenecks.
- **Predictable Performance :** Since the block generation cycle remains Deterministic rather than probabilistic, we guarantee predictable network performance (SLA) essential for enterprise application operation.

6.3 Cryptographically Verifiable Authority

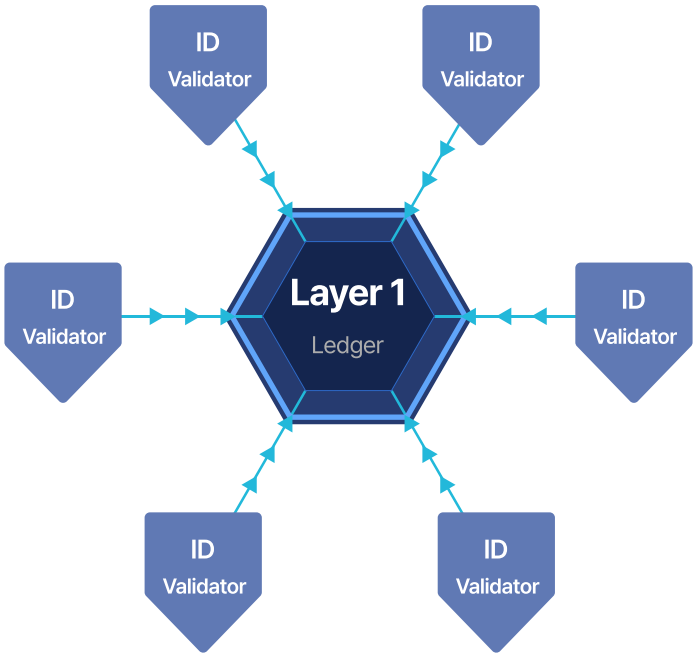
While existing PoA relied on centralized reputation, Quantarium's PoA presents a trust model combined with PQC technology.

- **QUANTA-X & SPHINCS+ Based Identity Proof :** All validator nodes must prove their identity with a SPHINCS+ key pair generated via the QUANTA-X engine when participating in the network. This means the validator's **Authority** is based on mathematically verifiable **Digital Signatures**, not vague social credit.
- **Verifiable Authority Delegation :** The reliability of consensus participants is transparently guaranteed by governance rules specified in smart contracts and cryptographic evidence on-chain, not by the arbitrary judgment of a central agency.
- **Accountability :** Since block generators sign blocks with their private keys, this provides clear accountability to immediately identify and **Slash** (remove) nodes in the event of malicious behavior.

6.4 Balance of Pragmatism and Security

In conclusion, Quantarium's Layer 1 PoA architecture is the optimal answer to catch two birds with one stone: the '**Extreme Security**' of quantum resistance and the '**Pleasant Speed**' required by commercial services. We provide a high-efficiency blockchain environment capable of accommodating real-world businesses without compromising the ideology of decentralization through a cryptographically verified authority model.

Quantarium PoA Consensus Architecture



7. PoA Governance & Validator Policy

On-Chain Governance Based on Transparency and Accountability

Quantarium's governance model combines the flexibility of a decentralized network with the strict control required by enterprise environments. We exclude irresponsible consensus participation based on anonymity and operate the network based on mathematically verified identities and clear protocol rules.

7.1 Trust-Based Entry Barriers: Validator Qualification

To become a **Validator** on the Quantarium network, strict technical and legal standards must be met beyond simple capital (Stake) deposits.

- **PQC-Based Cryptographic Identity Binding :** Prospective validators must register a SPHINCS+ key pair generated via the QUANTA-X engine on the network. This cryptographically specifies the operating entity of the node and guarantees that all future block generation activities are performed under that entity's signature.
- **Infrastructure Integrity Verification :** Nodes must have high-performance hardware specs and **HSM** (Hardware Security Module) integration environments that guarantee 24/7 **Availability**, which is pre-verified through performance benchmarks in the testnet phase.
- **KYC/KYB Verification :** To prevent anonymous attackers from taking over the network, a procedure is undergone to verify the existence of the operating entity (corporation, etc.) through the Foundation or Governance Committee.

7.2 Accountability Enhancement Mechanisms: Slashing & Automatic Revocation

Immediate and automated sanctions are applied by smart contracts for actions that undermine network trust. This builds trust based on the 'system' rather than 'goodwill.'

- **Double Signing Detection :** Signing two or more different blocks at the same block height is a critical attack that can cause a **Fork.** This is detected in real-time using the uniqueness of the SPHINCS+ signature, and upon detection, the node's authority is immediately suspended.
- **Downtime :** If a node fails to generate a block in the designated order or delays network synchronization, it is temporarily excluded from the consensus group or disqualified by a warning accumulation system **(Reputation Score).**
- **Slashing :** The deposit (**Stake**) posted by the validator is burned or converted to a damage compensation fund if malicious behavior is proven. This provides deterrence based on economic incentives.

7.3 Transparent On-Chain Governance Process

All policy changes in Quantarium are decided transparently on the blockchain, not in opaque meeting rooms.

- **Proposal & Voting :** Key network parameters such as **Gas Fee** policies, block size adjustments, and PQC parameter updates are changed through voting by the validator group. All voting records are permanently stored on the ledger and are auditable.
- **Emergency Security Protocol :** In case urgent security threats are detected, such as rapid advancements in quantum computer technology, a rapid response system is in place to immediately apply security patches or switch the network to '**Safe Mode**' with the consent of more than 2/3 of all validators.

7.4 Compliance & Auditability

This governance structure removes 'uncertainty,' the biggest barrier financial institutions and the public sector face when adopting blockchain.

- **Clarification of Legal Liability :** Since all transactions and blocks are processed by identity-verified validators, legal liability can be clearly attributed in case of issues.
- **Real-Time Audit Trails :** Regulatory authorities or external auditors can monitor the network operation status and fund flows in real-time by querying blockchain data without separate complex procedures.

8. Smart Contracts in PQC Environment

Separation of Execution Integrity and Access Control

Quantarium's smart contract architecture focuses on **"Execution Safety"** rather than "Language Complexity." We reject the notion that **Post-Quantum Cryptography (PQC)** functions must be inherent in the contract code syntax itself. Instead, we take a practical approach of clearly separating **Access Control** and **Execution Logic.**

8.1 PQC Location: Auth Layer, Not Language Syntax

The Language used to write smart contracts in Quantarium does not itself contain quantum mechanical algorithms or complex cryptographic operations. This is to lower the entry barrier for developers and embrace the existing development ecosystem.

- **Signature-Based Entry Barrier :** Quantum resistance is provided at the moment the smart contract is **Called**, i.e., at the **Authentication Layer**. Any transaction attempting to execute a contract function must pass a **SPHINCS+** based signature to enter the EVM (or execution engine).
- **Separation of Logic and Security :** Developers focus only on implementing business logic (DeFi, NFT, etc.), while the security regarding who can execute that logic is fundamentally guaranteed by Quantarium's Core Layer through PQC signatures.

8.2 Ease of Security Auditing

Introducing new and obscure programming languages for PQC implementation can actually become a risk factor increasing potential bugs and vulnerabilities.

- **Compliance with Verified Standards :** Quantarium provides a smart contract execution environment that meets industry standards, allowing existing **Audit Tools** and **Formal Verification** methodologies to be applied as is.
- **Code Readability :** Smart contract code must be easy for humans to read and understand. By abstracting complex cryptographic operations to the system level, **Auditors** can focus only on logic flaws, increasing the efficiency and accuracy of audits.

8.3 Execution Predictability

In an enterprise environment, smart contract results must be Deterministic.

- **Isolated Sandbox :** Smart contracts are executed in a sandbox environment completely isolated from the consensus engine and PQC crypto modules. This blocks infinite loops or errors in specific contracts from affecting the consensus process of the entire network.
- **Clarity of Gas Costs :** By calculating PQC signature verification costs and logic execution costs separately, users can accurately predict the costs required for transaction execution in advance.

9. Ecosystem Overview

Unified Quantum-Resilient Security Loop

The Quantarium ecosystem is not a simple collection of individual services. It is a structure where the four elements of the digital economy(**Wallet, Payment, Communication, and Asset Transfer**)are organically integrated within a single unbroken '**Quantum-Resilient Security Loop**'

9.1 Shared PQC Security Philosophy

All applications (dApps) and infrastructure within the ecosystem share the same security philosophy : **"Secure from End-to-End"**

- **Uniformity of Security :** From the moment a user creates a wallet, to chatting via messenger, transferring assets, and completing payments, the same security strength based on the **NIST Standard SPHINCS+** is applied to the entire process. This means there are no **'Weak Links'** where security levels drop when moving between services.
- **Consistency of User Experience (UX) :** Complex PQC key management and signing processes are handled in the background, allowing users to experience a consistent and intuitive interface throughout the ecosystem.

9.2 Core Ecosystem Components

1. **Quantum-Resistant Wallet :** The gateway to the ecosystem responsible for the safe generation and storage of PQC Key Pairs. It supports Cold Storage and Multi-Signature functions to fundamentally block asset theft.
2. **SECURET (Secure Communication) :** Beyond a simple messenger, this is an encrypted communication channel linked to wallet addresses. It protects financial information and sensitive personal data by transmitting messages that are indecipherable even by quantum computers.
3. Asset Bridge: A passage for safely bringing assets from other blockchains to the Quantarium network. It performs PQC verification even during the bridging process to block the inflow of external threats.

9.3 Structural Isolation & Containment

The Quantarium ecosystem is highly connected but strictly **Compartmentalized** in terms of security.

- **Blocking Vulnerability Spread :** Even if logic vulnerabilities are discovered in a specific dApp or component within the ecosystem, the design prevents this from spreading to the consensus algorithm of the Quantarium mainnet or the security of other assets.
- **Modular Security :** Since each component communicates with the Core Layer through independent security modules, the system possesses robust **Resilience** where failures in individual services do not lead to **Systemic Failure.**

10. Quantarium Dual Token Economy

10.1 Overview

The Quantarium ecosystem has adopted a 'Dual Token Structure' that separates QTA, the infrastructure asset of the mainnet, and QX, the utility asset of the exchange ecosystem, to simultaneously secure technical stability and economic liquidity. This design protects the mainnet's security and gas fee policies from being threatened by market volatility while providing a foundation for the exchange-centered independent economic ecosystem to grow flexibly.

10.2 Quantarium Mainnet Coin: QTA

(1) Definition and Role

QTA (Quantarium Coin) is the Native Asset of the Quantarium Post-Quantum Cryptography (PQC) mainnet. It is used as the base currency for paying all transaction fees (Gas Fees) within the network, executing smart contracts, and participating in the consensus of Validator nodes.

(2) Supply & Burn Model

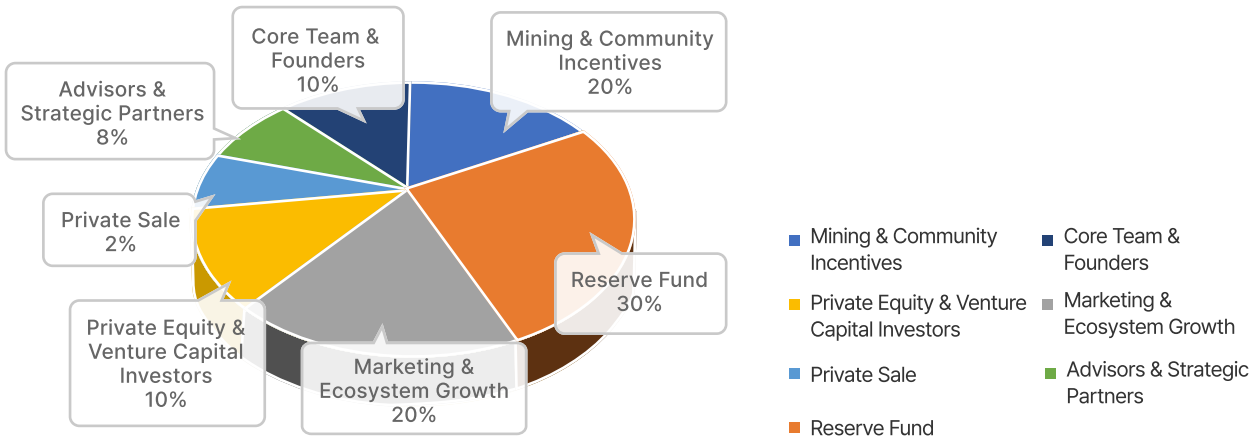
- **Total Supply:** 100 Billion QTA (100,000,000,000 QTA)
- **Deflationary Model (Automatic Burn Mechanism) :** QTA is equipped with an algorithm where a certain portion of the gas fee is automatically burned in proportion to network usage. This forms a deflationary structure where the circulating supply decreases as the ecosystem becomes active, increasing the coin's scarcity value.

(3) QTA Initial Allocation

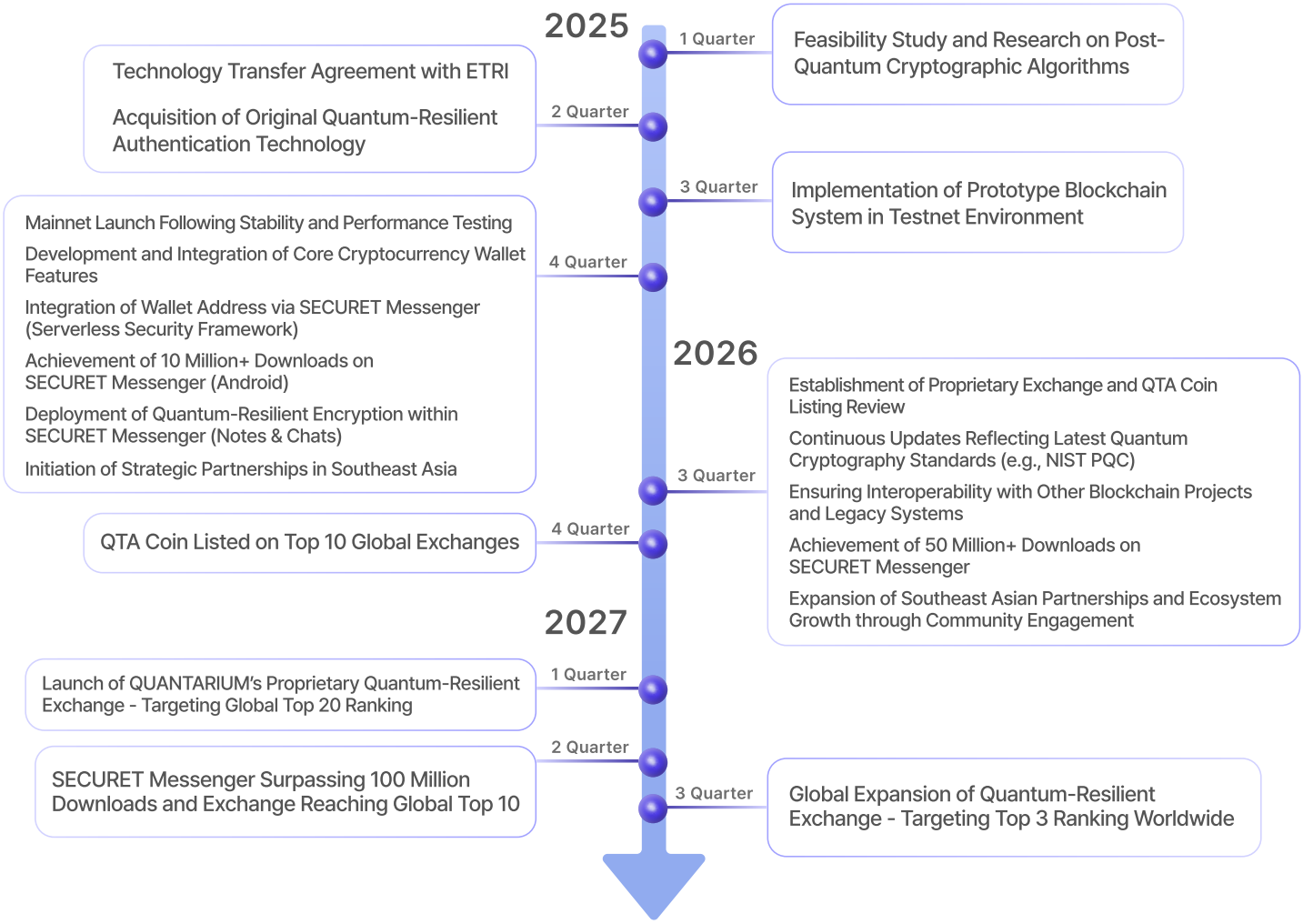
The Quantarium Foundation has strategically allocated the volume for long-term ecosystem operation and decentralization as follows.

Category	Allocation (%)	Token Amount, QTA	Description
Core Team & Founders	10%	10,000,000,000	Allocated as compensation for the development and founding team for the long-term operation, technical maintenance, and strategic governance of the QUANTARIUM network.
Advisors & Strategic Partners	8%	8,000,000,000	Distributed to legal, technical, and business advisory groups supporting ecosystem development, regulatory compliance, and global partnership expansion.
Marketing & Ecosystem Growth	20%	20,000,000,000	Used for marketing activities for QUANTARIUM Coin adoption and ecosystem expansion, such as user acquisition, global branding, and community activation.
Private Equity & Venture Capital Investors	10%	10,000,000,000	Allocated to institutional and strategic investors supporting ecosystem liquidity and technical expansion in the early stages.
Private Sale	2%	2,000,000,000	A limited pre-sale for accredited investors, forming the initial market and raising project funds.
Mining & Community Incentives	20%	20,000,000,000	Used to promote decentralized verification and ecosystem contribution, such as mining rewards, staking programs, and user participation incentives.
Reserve Fund	30%	30,000,000,000	Held as strategic reserves for maintaining network stability, R&D funds, establishing strategic partnerships, and securing emergency liquidity.
Total Supply	**100%**	**100,000,000,000**	

QTA Initial Allocation



QUANTARIUM ROAD MAP



10.3 Quantarium Exchange Utility Token: QX

(1) Definition and Features

QX (Quantarium Exchange Token) is the core utility token of the Quantarium Exchange built by the Quantarium Foundation. If QTA is the infrastructure fuel, QX has the character of a membership token that grants service access rights and benefits.

(2) Supply & Utility

- **Total Supply:** 1 Billion QX (1,000,000,000 QX), fixed quantity with no additional issuance.
- **Key Utilities:**

A. Transaction Fee Discount: Differential fee benefits based on QX holdings.

B. Launchpad Participation: Priority allocation for early tokens of promising projects.

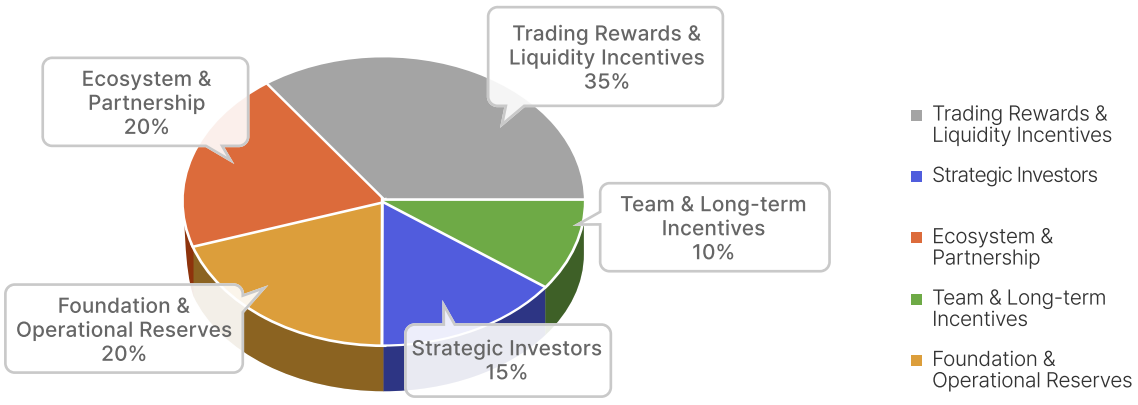
C. Governance Voting: Voting rights on listing reviews and major exchange policies.

D. PQC Security Integration: Application of the mainnet's PQC digital signature during transfers between user wallets and withdrawals to ensure quantum-resistant security.

(3) QX Distribution and Allocation Structure An allocation policy focused on liquidity supply and participant compensation in the exchange ecosystem is implemented.

Category	Allocation (%)	oken Amount, QX	Description
Trading Rewards & Liquidity Incentives	35%	350,000,000	Key resource for liquidity supply and trading activation. Trading contribution rewards, Liquidity Provider (LP) incentives, Staking rewards.
Ecosystem & Partnership	20%	200,000,000	Strategic budget for global expansion and usage expansion. Partnership expansion, Marketing & Community, Ecosystem fund.
Foundation & Operational Reserves	20%	200,000,000	Safety net supporting long-term survival and stable operation. Operational costs, Emergency reserves, R&D investment.
Strategic Investors	15%	150,000,000	Securing early funds, utilizing networks. Attracting VCs and institutional investors.
Team & Long-term Incentives	10%	100,000,000	Motivation for key personnel and talent acquisition. Rewards for core team and founders.
Total Supply	100%	1,000,000,000	

※ Strict Vesting and Lock-up policies apply to all team and investor volumes.



10.4 Structural Synergy between QTA and QX

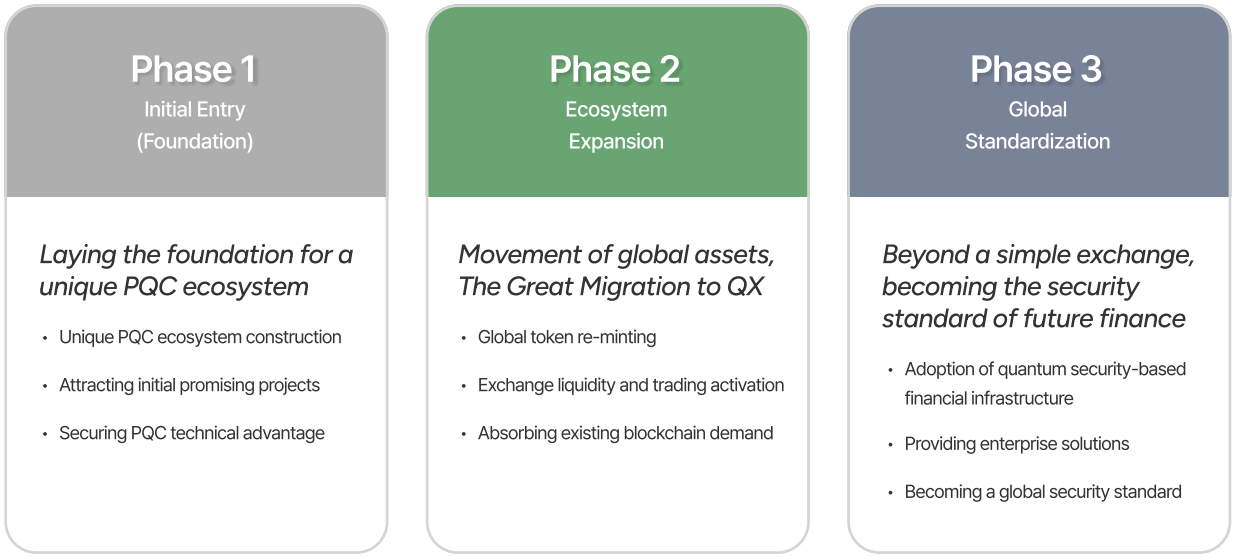
QTA and QX have clearly distinguished roles but operate in a complementary manner. The value of QTA rises in proportion to mainnet usage (transactions), while the value of QX is linked to the growth of the exchange platform and user expansion.

Comparison Item	QTA (Mainnet Coin)	QX (Exchange Token)
Nature	Mainnet Native Coin (Infrastructure)	Exchange Utility Token (Service)
Total Supply	100 Billion	1 Billion
Key Functions	Gas, On-chain execution, Consensus verification	Fee discount, Launchpad, Voting, VIP benefits
Value Driver	Automatic Burn, Network demand increase	Supply reduction (Lock-up), Platform revenue model
Security Tech	Native PQC Layer 1 Protection	PQC Signature integration on withdrawal/transfer

10.5 Market Potential and Outlook

The Quantarium Mainnet is a next-generation infrastructure that structurally solves the **'Quantum Security Threat'** that existing blockchains have failed to address. Considering the current market capitalization of the blockchain market and the increasing trend in demand for quantum security technology, the Quantarium ecosystem has the following growth potential.

- **Rise of Security Premium:** As the threat of quantum computers becomes visible after 2026, the demand for 'Digital Migration'—moving assets and projects from existing ECDSA-based mainnets to the PQC-based Quantarium mainnet—is expected to surge.
- **Valuation Scenario:** A phased increase in corporate value is expected, from a conservative outlook upon initial ecosystem settlement to an optimistic scenario where it establishes itself as a global standard mainnet.



This outlook is not a mere expectation but an analysis based on changing global security standards (NIST, etc.) and structural market demand.

11. Conclusion

Immutable Trust for the Quantum Era

The history of digital assets has been a process of technically implementing 'trust.' However, the incoming wave of **Quantum Computing** fundamentally threatens the trust structure of the past decades that relied on existing cryptographic systems (RSA, ECC).

Concluding the **Quantarium** white paper, we wish to clearly redefine our technical direction once again and present our vision for the future.

10.1 Identity of Quantarium: Clarification

Many people experience confusion stemming from the word 'Quantum.' Therefore, Quantarium clearly defines our technical essence as follows :

> **"Quantarium is not a blockchain that uses quantum computers.""Quantarium is a blockchain that survives even in the quantum computing era."**

We are not hardware that performs calculations using quantum mechanical phenomena (superposition, entanglement). Quantarium is a software protocol armed with '**Post-Quantum Cryptography**' — the only shield capable of blocking quantum computers when they pierce existing security like a spear. We are not an attack tool, but a **Defense System protecting humanity's digital assets.**

10.2 Structural Resilience Beyond Uncertainty

The '**Harvest Now, Decrypt Later**' attack scenario is a present crisis, not a future threat. To counter this, Quantarium has adopted the **NIST Standard SPHINCS+**. Through a hash-based structure unaffected by the collapse of specific mathematical hard problems (like integer factorization), we have secured **Structural Resilience** that guarantees system safety regardless of the speed of quantum computer development or changes in algorithms.

10.3 Pragmatic Innovation: Coexistence of Security and Speed

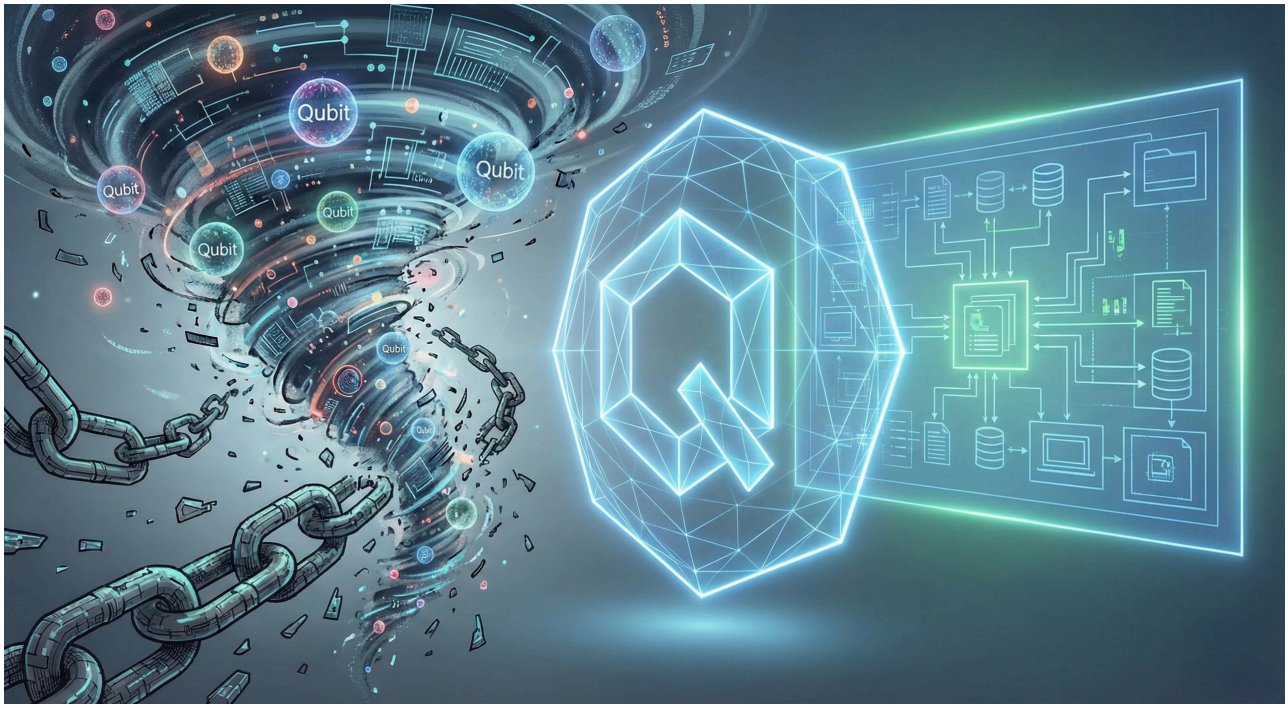
Past security enhancement technologies inevitably accompanied performance degradation. However, Quantarium has solved this dilemma by combining an **Independent Layer 1 Architecture** with the **PoA (Proof of Authority)** consensus algorithm. Through cryptographically verified trust nodes, we have absorbed the heavy computational load of post-quantum cryptography and realized **Instant Finality** and high-speed transactions required by enterprise environments. This means Quantarium is ready to support the real-world economy, moving beyond the theoretical laboratory.

10.4 Closing: The Digital Noah's Ark

Technological advancement is a blessing, but it can be a disaster for those who are unprepared. When the era of **Quantum Supremacy** arrives and the defenses of legacy blockchains crumble, Quantarium will become the **'Digital Noah's Ark'**, safely preserving value and carrying it into the future.

The Quantarium ecosystem has integrated the entire process of wallet, payment, communication, and asset transfer into one powerful PQC security loop. Now, we propose to developers, enterprises, and all users: Design an unshakable future together on the safest foundation.

Quantarium does not wait for the future to come. We are ready to endure that future.



12. References

The security architecture, post-quantum cryptographic standards, and consensus algorithms of Quantarium described in this white paper were designed based on the following international standards, academic papers, and technical reports.

1. National Institute of Standards and Technology (NIST). (2016–2024). *Post-Quantum Cryptography Standardization. U.S. Department of Commerce.*
2. National Institute of Standards and Technology (NIST). (2024). *FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA). U.S. Department of Commerce.*
3. Bernstein, D. J., Hülsing, A., et al. (2019). *SPHINCS+: Submission to the NIST Post-Quantum Cryptography Project.*

5. Mosca, M. (2018). *Cybersecurity in an Era with Quantum Computers. IEEE Security & Privacy.*
6. Shor, P. W. (1994). *Algorithms for Quantum Computation: Discrete Logarithms and Factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS).*
7. Grover, L. K. (1996). *A Fast Quantum Mechanical Algorithm for Database Search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC).*
8. Barker, E. *Digital Signature Standard (DSS). NIST FIPS 186-5. National Institute of Standards and Technology.*
9. Kahn Academy / IBM Research. *Quantum Computing and Cryptography Overview.*
10. European Union Agency for Cybersecurity (ENISA). (2021). *Post-Quantum Cryptography : Current State and Quantum Mitigation.*
11. National Security Agency (NSA). (2022). *Commercial National Security Algorithm Suite 2.0 (CNSA 2.0).*
12. ISO/IEC JTC 1/SC 27. *IT Security Techniques – Cryptographic Algorithms. International Organization for Standardization.*
13. Buterin, V. *On Public and Private Blockchains. Ethereum Research.*
14. Wood, G. *Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Yellow Paper.*
15. BFT Consensus Research. *Authority-based Consensus Mechanisms in Permissioned Blockchains.*