세계 최초의 양자 내성 블록체인을 통한 분산 원장 기술로
원치않는 해킹으로부터 자유를! 기기 간에 빠른 소통을!

Quantarium

White paper v2.1
백서 한국어판

Steve Jung
공동 창립자, CEO

Quantarium Coin White Paper

CONTENTS

1. 서문 (Executive Summary)

1.1 프로젝트 개요: 태생적 양자내성 블록체인의 필요성
(Project Overview: The Necessity of Native Quantum-Resistant Blockchain)

디지털 경제의 기반이 되는 암호학적 신뢰(Cryptographic Trust)는 현재 중대한 전환점에 직면해 있습니다. 지난 수십 년간 인터넷과 블록체인 산업을 지탱해 온 **RSA** 및 **타원곡선암호(ECC/ECDSA)** 체계는 양자컴퓨팅(Quantum Computing)의 비약적인 발전으로 인해 그 수학적 난제인 소인수분해와 이산로그 문제의 계산 복잡도가 붕괴될 위기에 처해 있습니다.

오류 정정 큐비트(Logical Qubit)의 실질적 구현과 하이브리드 양자 알고리즘의 발전은 '양자 우위(Quantum Supremacy)'의 도래 시점을 앞당기고 있으며, 이는 기존 공개키 기반 구조(PKI)에 의존하는 모든 블록체인 네트워크에 실존적인 위협이 되고 있습니다. 특히, 현재의 암호화된 데이터를 공격자가 수집해 두었다가 미래의 양자컴퓨터로 해독하는 **'선 수집 후 해독(Harvest Now, Decrypt Later)'** 공격 시나리오는 미래가 아닌 현재의 시급한 보안 문제입니다.

현존하는 대부분의 블록체인(Bitcoin, Ethereum 등)은 양자내성(Post-Quantum Cryptography, PQC)을 고려하지 않고 설계되었습니다. 향후 소프트포크 등을 통해 PQC 서명으로 업그레이드한다 하더라도, 과거에 생성된 제네시스 블록부터 업그레이드 시점 전까지의 모든 트랜잭션 기록은 여전히 취약한 구형 암호 체계로 남아 있게 됩니다. 이를 **'양자 레거시 취약성(Quantum Legacy Vulnerability)'**이라 정의하며, 이는 자산의 영구적 소유권을 보장해야 하는 블록체인의 본질적 가치를 훼손합니다.

퀀타리움(Quantarium)은 이러한 구조적 딜레마를 해결하기 위해 탄생했습니다. 퀀타리움은 기존 체계에 양자내성 기능을 덧붙이는 사후적 접근을 거부합니다. 대신, 네트워크의 시작점인 제네시스 블록(Genesis Block)부터 모든 트랜잭션, 서명, 검증 과정에 양자내성 암호 알고리즘을 적용한 **'태생적(Native) 양자내성 Layer 1 블록체인'**입니다. 퀀타리움은 양자 시대에도 변하지 않는 데이터의 무결성과 자산의 안전성을 보장하는 차세대 디지털 신뢰 인프라의 표준을 제시합니다.

1.2 퀀타리움의 핵심 가치 제안 (Core Value Proposition)

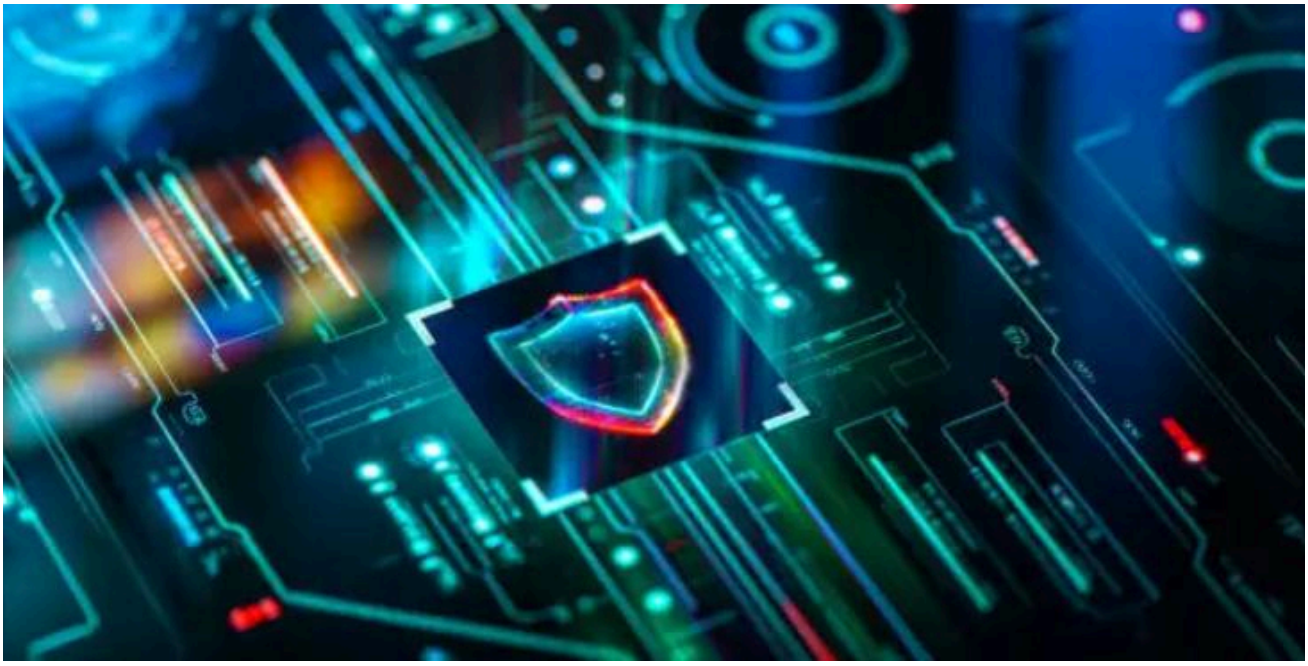
퀀타리움은 단순한 기술적 실험이 아니며, 엔터프라이즈 및 공공 인프라 수준의 요구사항을 충족하는 실용적인 블록체인 솔루션입니다. 우리의 핵심 가치는 다음 네 가지 축으로 정의됩니다.

- **NIST 표준 기반의 신뢰성 (Standard Compliance):** 퀀타리움은 독자적이거나 검증되지 않은 암호 알고리즘을 사용하지 않습니다. 우리는 미국 국립표준기술연구소(NIST)가 양자내성 전자서명 표준으로 최종 선정한 **SPHINCS+** 계열의 알고리즘을 핵심 보안 엔진**(QUANTA-X)**으로 채택했습니다. SPHINCS+는 수학적 난제에 의존하지 않는 완전 해시 기반(Hash-based) 서명 방식을 사용하여, 미지의 수학적 공격 기법이 발견되더라도 무너지지 않는 가장 보수적이고 확실한 안전성을 제공합니다.

- **레거시 없는 무결성 (Legacy-Free Integrity):** 설계 단계부터 PQC가 적용된 'Native Layer 1' 구조는 과거 데이터에 대한 소급적 해킹 위협을 원천 차단합니다. 이는 장기적인 가치 보존이 필요한 금융 자산, 부동산 토큰화(RWA), 국가 기록물 관리 등 초장기적 신뢰가 요구되는 분야에 유일한 해답을 제공합니다.

- **엔터프라이즈급 성능과 합의 (High Performance & Consensus):** 보안이 성능 저하를 의미해서는 안 됩니다. 퀀타리움은 **권한 증명(Proof of Authority, PoA)** 합의 메커니즘을 도입하여 불필요한 채굴 경쟁을 제거했습니다. 신원이 검증된 노드(Validator)를 통해 높은 처리량(Throughput)과 즉각적인 파이널리티(Finality)를 보장함으로써, 실시간 결제 및 대규모 트랜잭션 처리가 가능한 상용 환경을 구축했습니다.

- **통합된 보안 생태계 (Unified Security Ecosystem):** 퀀타리움은 블록체인 네트워크를 넘어선 **'양자내성 보안 루프(Quantum-Resilient Security Loop)'**를 제공합니다. 사용자의 개인키 생성부터 자산 전송(Wallet), 네트워크 합의(Consensus), 그리고 데이터 통신(SECURET Messenger)에 이르기까지 전 과정에 동일한 PQC 보안 스택을 적용하여, 시스템 내 단일 실패 지점(Single Point of Failure)을 제거한 완결된 보안 환경을 제공합니다.



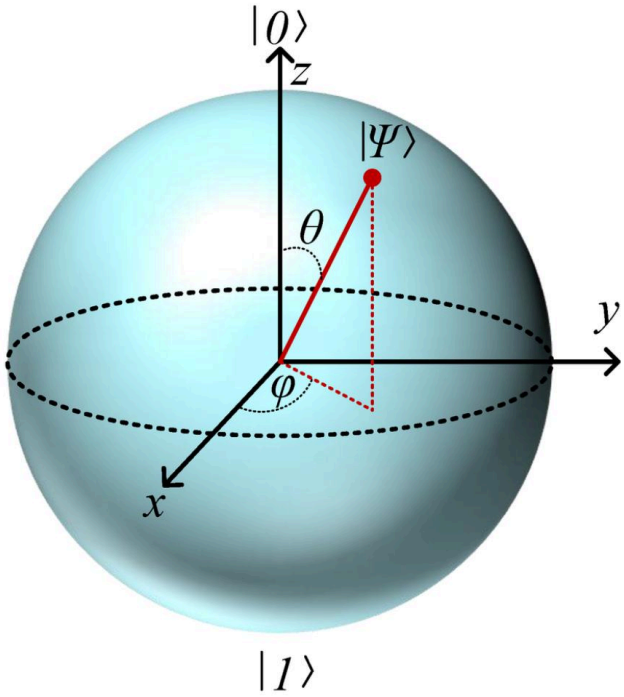
2. 시장 배경 및 위협 모델 (Market Context & Threat Model)

2.1 양자컴퓨팅의 발전 현황과 암호학적 위기
(Advancement of Quantum Computing & The Cryptographic Crisis)

현대 정보 기술(IT) 인프라는 0과 1의 비트(Bit) 기반 연산을 수행하는 고전 컴퓨터의 한계 내에서 설계된 암호 체계에 의존하고 있습니다. 그러나 양자역학의 원리인 중첩(Superposition)과 얽힘(Entanglement)을 이용하는 **양자컴퓨팅(Quantum Computing)** 기술의 비약적인 발전은 이러한 전제를 근본적으로 뒤흔들고 있습니다.

최근 IBM, Google, Quantinuum 등 주요 기술 기업들은 수백 큐비트(Qubit) 급의 프로세서를 넘어, 오류 정정(Error Correction)이 가능한 **'논리 큐비트(Logical Qubit)'** 단계로 진입하고 있습니다. 이는 양자컴퓨터가 실험실 수준을 벗어나 실질적인 연산 능력을 갖춘 상용화 단계로 진입했음을 시사합니다.

암호학적 관점에서 이러한 발전은 '위기'로 정의됩니다. 현대 공개키 기반 구조(PKI)의 안전성은 '큰 수의 소인수분해'나 '이산로그 문제'를 해결하는 데 천문학적인 시간이 소요된다는 **계산 복잡도(Computational Complexity)** 가정에 기반합니다. 그러나 쇼어 알고리즘(Shor's Algorithm)을 탑재한 양자컴퓨터는 이러한 수학적 난제를 다항 시간(Polynomial Time) 내에 해결할 수 있어, 기존 인터넷 통신과 금융 거래를 지탱하던 보안의 둑을 무너뜨릴 잠재력을 가지고 있습니다.



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

2.2 기존 블록체인(RSA/ECC 기반)의 구조적 붕괴 위험

(Structural Collapse Risk of Legacy Blockchains based on RSA/ECC)

블록체인 기술의 핵심은 탈중앙화된 신뢰이며, 이 신뢰는 디지털 서명(Digital Signature)을 통해 보장됩니다. 비트코인(Bitcoin), 이더리움(Ethereum)을 포함한 현존하는 대다수의 메이저 블록체인 네트워크는 **타원곡선 암호(ECC)**, 구체적으로는 **ECDSA(Elliptic Curve Digital Signature Algorithm)** 또는 **RSA** 알고리즘을 사용합니다.

양자 우위(Quantum Supremacy) 시대가 도래할 경우, 이러한 레거시 블록체인은 다음과 같은 구조적 붕괴 위험에 직면합니다.

1. **공개키 역산 및 지갑 탈취** : 쇼어 알고리즘을 이용하면 블록체인 상에 공개된 공개키(Public Key)로부터 사용자의 개인키(Private Key)를 도출해낼 수 있습니다. 이는 공격자가 정당한 소유자 몰래 자산을 전송하거나 스마트 컨트랙트 권한을 탈취할 수 있음을 의미합니다.
2. **트랜잭션 위변조** : 타원곡선 이산로그 문제(ECDLP)가 무력화되면, 공격자는 유효한 전자서명을 위조할 수 있습니다. 이는 블록체인의 무결성(Integrity)을 파괴하고 이중 지불(Double Spending) 공격을 가능케 하여 네트워크의 경제적 가치를 '0'으로 수렴시킬 수 있습니다.
3. **합의 알고리즘 마비** : PoS(지분 증명) 등의 합의 과정에서도 검증자의 서명이 필수적입니다. 서명 체계가 뚫리면 네트워크 전체의 합의를 조작하거나 마비시킬 수 있습니다.
4. **해시 알고리즘의 보안 강도 저하 (Weakening of Hash Algorithms via Grover's Algorithm)**쇼어 알고리즘(Shor's Algorithm)이 비대칭 키 암호(전자서명)를 무력화한다면, 그로버 알고리즘(Grover's Algorithm)은 블록체인의 연결 구조와 무결성을 보장하는 해시 함수(Hash Function)를 위협합니다.

- **양자 가속과 보안 수준 반감** : 그로버 알고리즘은 비정형 데이터 검색 속도를 양자적으로 가속화(Quadratic Speedup)하여, 해시 함수의 충돌 저항성(Collision Resistance)을 약화시킵니다. 이론적으로 이는 현재 사용되는 SHA-256 등의 해시 알고리즘 보안 강도를 절반 수준(128비트)으로 떨어뜨리는 효과를 가져옵니다.
- **대응의 차이점** : 해시 함수의 경우 출력 길이를 늘리는 방식(예: SHA-256 → SHA-512)으로 양자 위협에 대한 방어가 일정 부분 가능합니다. 그러나 전자서명(ECDSA)은 쇼어 알고리즘에 의해 수학적 난제 자체가 붕괴되므로, 단순한 키 길이 확장으로는 방어가 불가능하며 **양자내성 암호(PQC)로의 전면적인 알고리즘 교체**만이 유일한 해결책입니다.

5. **결론 : 구조적 전환의 불가피성 (Inevitability of Structural Transition)**결과적으로 기존 블록체인은 지갑 보안과 소유권을 증명하는 전자서명 영역에서 '존재론적 위협(Existential Threat)'에 직면해 있습니다. 따라서 블록체인의 지속 가능한 보안을 위해서는 기존 체계의 점진적 수정이 아닌, 설계 단계부터 PQC 전자서명을 탑재한 인프라로의 구조적 전환이 필수적입니다.

2.3 'Harvest Now, Decrypt Later' 공격과 레거시 취약성
(HNDL Attack & Legacy Vulnerability)

양자컴퓨터가 상용화되지 않은 현재 시점에서도 보안 위협은 실재합니다. 바로 '**선 수집 후 해독(Harvest Now, Decrypt Later, HNDL)**' 공격 시나리오 때문입니다.

1. **공격 메커니즘** : 해커나 적대적 국가 기관은 현재의 암호화 기술로 보호된 데이터(트랜잭션 기록, 통신 패킷 등)를 지금 해독하지 못하더라도 대량으로 수집하여 저장합니다. 그리고 수년 후 충분한 성능의 양자컴퓨터가 개발되었을 때 이를 일괄적으로 해독합니다.
2. **블록체인의 딜레마 (Immutability Paradox)** : 블록체인의 '불변성'은 이 공격 시나리오에서 치명적인 약점이 됩니다. 블록체인에 한 번 기록된 데이터는 삭제하거나 수정할 수 없습니다. 따라서 현재 RSA/ECC 기반으로 생성된 트랜잭션 기록은 미래에 영구적으로 노출될 운명에 처해 있습니다.
3. **레거시 취약성** : 기존 블록체인이 향후 소프트포크를 통해 PQC로 업그레이드하더라도, 업그레이드 이전에 생성된 과거의 주소와 트랜잭션은 여전히 구형 알고리즘으로 서명되어 있습니다. 공격자는 이 과거 데이터를 통해 초기 진입점(Entry Point)을 확보하거나, 장기간 이동하지 않은 자산(Sleeper Wallets)을 탈취할 수 있습니다. 이를 '양자 레거시 취약성'이라 하며, 사후적 대응으로는 해결할 수 없는 근본적 문제입니다.

2.4 양자내성(PQC) 전환의 시급성 및 글로벌 표준 동향
(Urgency of PQC Transition & Global Standardization)

양자 위협에 대응하기 위한 글로벌 표준화 작업은 이미 '준비' 단계를 넘어 '이행' 단계로 접어들었습니다.

- **NIST 표준화 완료** : 미국 국립표준기술연구소(NIST)는 2016년부터 진행해 온 양자내성암호 공모전을 통해 2024년 8월, **SPHINCS+(SLH-DSA)**, Kyber(ML-KEM), Dilithium(ML-DSA)을 최종 표준 알고리즘(FIPS)으로 공식 발표했습니다. 이는 PQC가 실험적 기술이 아닌, 산업 표준임을 확정 짓는 사건입니다.
- 각국 정부의 의무화: 미국 백악관은 국가안보각서(NSM-10)를 통해 모든 연방 기관의 시스템을 2035년까지 PQC로 전환할 것을 지시했으며, NSA(국가안보국) 역시 CNSA 2.0 스위트를 발표하며 전환을 독려하고 있습니다.
- 시급성: 시스템 마이그레이션에는 통상 수년 이상의 시간이 소요됩니다. 양자컴퓨터의 발전 속도가 예상보다 빠를 수 있다는 점(Y2Q 문제)을 고려할 때, 지금 즉시 PQC를 도입하지 않는 시스템은 미래의 기술 부채(Technical Debt)가 아닌 '보안 파산' 상태에 이르게 될 것입니다.

따라서, **NIST 표준인 SPHINCS+를 탑재한 퀀타리움의 등장은 단순한 기술적 진보가 아니라, 변화하는 글로벌 보안 표준에 부합하는 유일하고 시급한 대안**입니다.

3. 퀀타리움 솔루션 및 설계 철학 (Solution & Philosophy)

퀀타리움(Quantarium)은 기존 블록체인의 한계를 극복하기 위한 점진적 개선(Incremental Improvement)이 아닌, 양자 컴퓨팅 시대의 도래라는 패러다임 전환에 대응하기 위한 **근본적 재설계(Fundamental Redesign)**입니다. 우리의 솔루션은 보안을 타협 불가능한 최우선 가치로 설정하며, 이를 구현하기 위해 **태생적 양자내성(Native PQC)**과 **NIST 표준 준수**라는 두 가지 핵심 축을 기반으로 설계되었습니다.

3.1 설계 원칙: 보안 우선성(Security-First)과 불변성
(Design Principles: Security-First & Immutability)

퀀타리움의 아키텍처는 모든 설계 단계에서 **'보안 우선성(Security-First)'** 원칙을 따릅니다. 이는 성능(Scalability)이나 편의성(Usability)을 위해 보안을 희생하지 않음을 의미합니다.

- **진정한 불변성(True Immutability)의 정의** : 기존 블록체인이 주장하는 불변성은 '현재의 컴퓨팅 파워'를 전제로 합니다. 그러나 양자컴퓨터의 연산 능력 앞에서도 데이터가 변하지 않고 보호받을 수 있어야 진정한 불변성이라 할 수 있습니다. 퀀타리움은 "현재 기록된 데이터는 미래의 어떤 기술적 진보에 의해서도 위변조될 수 없다"는 명제를 충족하도록 설계되었습니다.
- **제로 트러스트(Zero Trust) 기반 설계** : 우리는 네트워크 참여자뿐만 아니라, 미래의 컴퓨팅 환경조차 신뢰하지 않습니다. 따라서 잠재적인 암호 해독 기술의 발전을 가정하고, 가장 보수적이고 검증된 암호학적 방법론만을 적용하여 리스크를 최소화합니다.
- **장기적 데이터 생존성(Long-term Data Survivability)** : 금융 자산, 신원 정보, 공공 기록 등은 수십 년 이상 보존되어야 합니다. 퀀타리움은 단기적인 트랜잭션 처리 속도 경쟁보다는, 50년, 100년 후에도 데이터의 무결성을 보장하는 '디지털 영속성'을 목표로 합니다.

3.2 태생적 양자내성(Native PQC) 아키텍처
(Native Post-Quantum Cryptography Architecture)

많은 블록체인 프로젝트들이 기존 알고리즘(RSA/ECC) 위에 PQC를 덧붙이는 하이브리드(Hybrid) 방식이나 소프트포크를 통한 마이그레이션을 계획하고 있습니다. 그러나 퀀타리움은 제네시스 블록(Genesis Block)부터 PQC가 적용된 **'태생적(Native)'** 접근 방식을 취합니다.

- **레거시 제로(Zero Legacy)** : 기존 체인의 업그레이드 방식은 업그레이드 이전의 과거 데이터(Old Tx)가 구형 암호 체계로 남아있는 '레거시 취약점'을 남깁니다. 퀀타리움은 시작점부터 양자내성 알고리즘을 적용하므로, 네트워크 전체 역사에서 양자 공격에 취약한 연결 고리(Weak Link)가 존재하지 않습니다.

- **전방위적 보안 적용 (Full-Stack Security)** : 양자내성은 특정 레이어에만 국한되지 않습니다.
    1. **Wallet Layer** : 주소 생성 및 키 관리 단계부터 PQC 적용.
    2. **Transaction Layer** : 자산 전송 서명 및 검증.
    3. **Consensus Layer** : 검증자 노드 간의 합의 메시지 및 블록 제안 서명. 이처럼 시스템의 모든 계층이 동일한 수준의 PQC 보안 강도로 보호됩니다.
- **Harvest Now, Decrypt Later 방어** : 태생적 PQC 아키텍처는 현재 수집되고 있는 암호화된 데이터 패킷조차 양자컴퓨터로 해독할 수 없도록 만듭니다. 이는 데이터의 기밀성과 무결성을 미래 시점까지 완벽하게 확장합니다.

3.3 NIST 표준 준수 및 구조적 회복력 확보 (NIST Standard Compliance & Structural Resilience)

독자적인 암호 알고리즘은 검증되지 않은 취약점을 내포할 위험이 있습니다. 퀀타리움은 글로벌 보안 표준을 준수하여 엔터프라이즈급 신뢰성을 확보했습니다.

- **NIST 표준 SPHINCS+ 채택** : 우리는 미국 국립표준기술연구소(NIST)가 양자내성 전자서명 표준으로 선정한 **SPHINCS+** 계열을 핵심 엔진으로 채택했습니다. 이는 전 세계 암호학계의 수년간에 걸친 검증(Public Review)을 통과한 알고리즘으로, 수학적 안전성이 입증되었습니다.
- **해시 기반 서명의 구조적 회복력** : SPHINCS+는 격자 기반(Lattice-based) 암호와 달리, 특정 수학적 난제(SVP 등)에 의존하지 않고 오직 **암호학적 해시 함수(Hash Function)의 보안성**에만 의존합니다. 이는 설령 미래에 새로운 수학적 파훼법이 발견되어 다른 PQC 알고리즘이 위협받더라도, 해시 함수가 안전한 한 시스템은 무너지지 않음을 의미합니다. 퀀타리움은 이러한 '구조적 회복력(Structural Resilience)'을 통해 최후의 보루와 같은 안전성을 제공합니다.
- **규제 호환성 (Regulatory Compatibility)** : NIST 표준의 채택은 향후 각국 정부 및 금융 규제 당국이 요구할 보안 가이드라인(예: CNSA 2.0)을 선제적으로 충족합니다. 이는 퀀타리움이 제도권 금융 및 공공 인프라로 채택되는 데 있어 결정적인 경쟁 우위를 제공합니다.

4. QUANTA-X: 핵심 양자내성 암호 엔진

퀀타리움(Quantarium)은 단일 암호 알고리즘의 적용을 넘어, 시스템 전체를 아우르는 포괄적인 'PQC 보안 스택(PQC Security Stack)'을 구축했습니다. 이 스택은 자체 개발된 QUANTA-X 엔진을 중심으로, NIST 표준 알고리즘인 SPHINCS+의 무결성과 상태 비저장(Stateless) 구조의 안정성을 결합하여 엔터프라이즈급 블록체인 인프라를 완성합니다.

4.1 QUANTA-X 엔진: 차세대 보안의 핵심 (QUANTA-X Engine: The Core of Next-Gen Security)

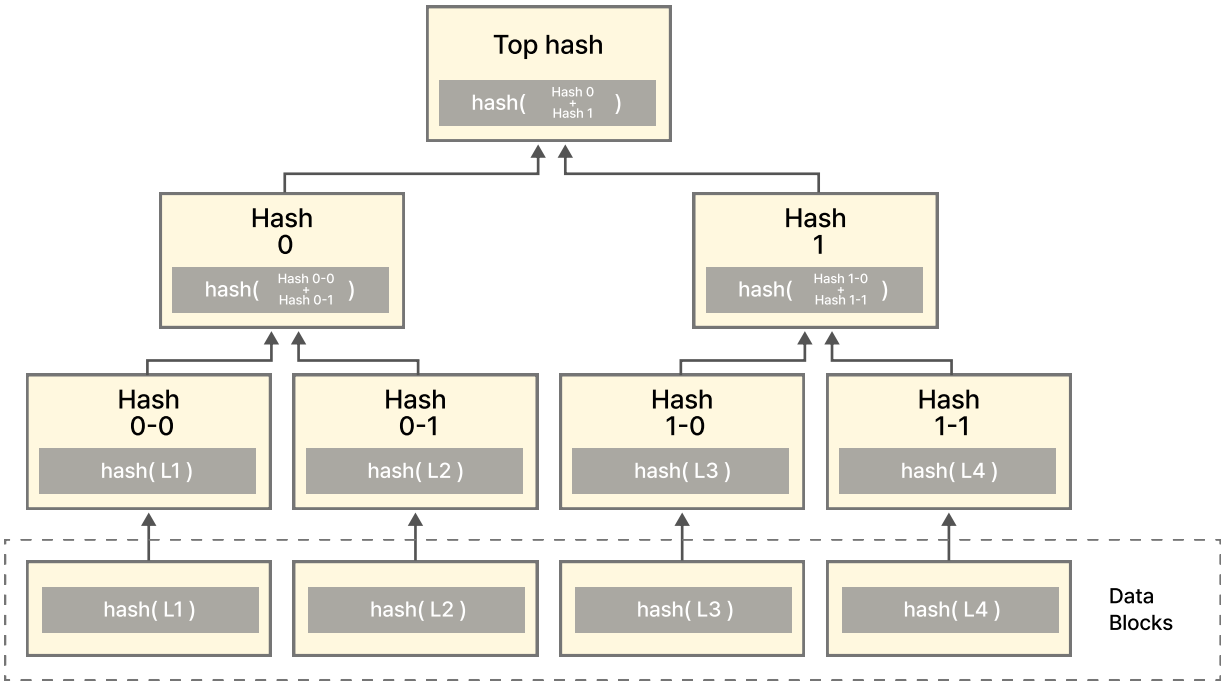
QUANTA-X는 퀀타리움 네트워크의 암호학적 연산을 전담하는 고성능 보안 엔진입니다. 단순한 알고리즘 라이브러리가 아닌, 블록체인 환경에 최적화된 통합 암호 모듈로서 다음과 같은 핵심 기능을 수행합니다.

- **하이브리드 키 관리 시스템 (KMS) :** 양자내성 키 쌍(Key Pair)의 생성, 저장, 로딩을 격리된 메모리 공간에서 처리하여 사이드 채널 공격(Side-Channel Attack)을 방어합니다.
- **서명 속도 최적화 (Signature Acceleration) :** 해시 기반 서명의 특성상 상대적으로 큰 서명 크기와 검증 시간을 블록체인의 실시간 처리 요구사항(Latency)에 맞게 최적화하는 가속화 로직을 포함합니다.
- **유연한 추상화 계층 (Abstraction Layer) :** 향후 암호학적 표준이 변경되거나 새로운 알고리즘(예: NIST Round 4 후보)이 등장하더라도, 하드포크 없이 엔진 레벨에서 유연하게 교체 및 업데이트가 가능한 모듈러(Modular) 구조를 갖추고 있습니다.

4.2 QUANTA-X 알고리즘: 완전 해시 기반 전자서명 (QUANTA-X Engine: The Core of Next-Gen Security)

퀀타리움은 미국 국립표준기술연구소(NIST)가 FIPS 205 표준으로 제정한 SPHINCS+ (SLH-DSA)를 메인넷의 기본 서명 알고리즘으로 채택했습니다. 이는 격자(Lattice) 기반 암호와 달리 수학적 난제에 의존하지 않는 가장 보수적이고 안전한 선택입니다.

- **보안 가정의 최소화 :** SPHINCS+의 보안성은 오직 '암호학적 해시 함수의 보안성(충돌 저항성 및 역상 저항성)'에만 의존합니다. 이는 소인수분해나 이산로그 문제는 물론, 격자 문제에 대한 파훼법이 미래에 발견되더라도 해시 함수(SHA-256/SHAKE)가 안전한 한 시스템은 뚫리지 않음을 의미합니다.
- **장기적 신뢰성 :** 특정 수학적 구조를 사용하지 않기 때문에, 양자 알고리즘의 발전 예측이 불확실한 상황에서 가장 리스크가 적은 'Fail-Safe' 솔루션으로 평가받습니다.
- **검증된 표준 :** 수년간의 전 세계 암호학자들에 의한 공개 검증(Public Review)을 거쳐 NIST 표준으로 확정된 알고리즘을 사용하여, 독자 알고리즘이 가질 수 있는 백도어나 설계 오류의 가능성을 원천 배제했습니다.



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

4.3 상태 비저장(Stateless) 구조를 통한 안정성 확보 (Stability via Stateless Architecture)

초기 해시 기반 서명(XMSS, LMS 등)은 키 사용 횟수를 기록해야 하는 **상태 기반(Stateful)** 방식이었습니다. 이는 '상태 동기화' 실패 시 동일한 일회용 키(OTS Key)를 재사용하게 되어 보안이 완전히 무너지는 치명적 단점이 있었습니다. 퀀타리움은 SPHINCS+의 **상태 비저장(Stateless)** 특성을 통해 이를 완벽히 해결했습니다.

- **다중 서명 및 백업 안전성 :** 사용자가 지갑을 백업 후 복구하거나, 클라우드 환경에서 가상 머신(VM)을 복제하더라도 '서명 카운트'를 관리할 필요가 없습니다. 이는 노드 운영의 복잡성을 제거하고 사용자 실수를 방지합니다.
- **FORS & WOTS+ 구조 :** SPHINCS+는 퓨레스트(Forest) 구조의 랜덤 해시 트리를 사용하여, 상태를 기억하지 않고도 확률적으로 키 재사용을 방지합니다. 이는 분산 원장 환경(Distributed Ledger)에서 필수적인 '비동기적 보안성'을 제공합니다.
- **무결성 보장 :** 수십억 건의 트랜잭션이 발생해도 서명 키의 보안 강도가 저하되지 않으며, 블록체인의 무중단 운영을 기술적으로 뒷받침합니다.

5. 퀀타리움 PQC 보안 스택 (Quantarium PQC Security Stack)

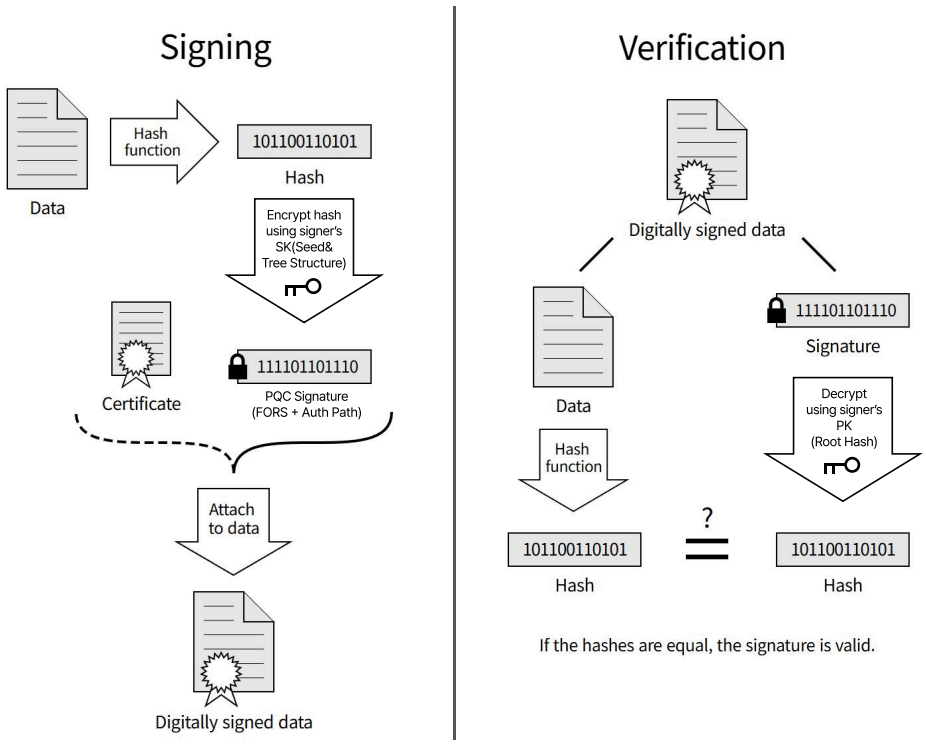
NIST SPHINCS+ 구현 및 암호학적 무결성

퀀타리움의 보안 스택은 네트워크 아키텍처 내부에서 작동하는 순수 암호 엔진과 프로토콜의 집합체입니다. 우리는 NIST 표준인 SPHINCS+를 단순 도입하는 것을 넘어, 이를 블록체인 환경의 제약 사항(저장 공간, 연산 속도)에 맞게 최적화하고 키 관리의 안전성을 극대화하는 독자적인 구현 기술을 적용했습니다.

5.1 SPHINCS+: 구조적 회복력을 갖춘 완전 해시 기반 서명
(SPHINCS+: Structural Resilience via Hash-Based Signature)

퀀타리움은 격자(Lattice) 기반 암호와 달리, 양자 컴퓨터 환경에서도 장기적인 암호 안전성을 제공하도록 설계된 SPHINCS+를 채택했습니다.

- **수학적 난제로부터의 독립** : SPHINCS+는 기존 공개키 암호(RSA, ECC)가 의존하는 소인수분해나 이산 로그 문제에 의존하지 않는 **완전한 해시 기반(Hash-Based) 포스트 퀀텀(Post-Quantum) 전자서명** 방식입니다.
- **구조적 회복력(Structural Resilience)** : 오직 암호학적 해시 함수의 보안성에만 의존하기 때문에, 특정 수학적 가정(Assumption)이 붕괴되더라도 시스템 전체의 보안이 무너지지 않습니다. 이는 미래 암호 환경의 불확실한 변화 속에서도 퀀타리움 네트워크가 생존할 수 있는 근본적인 내성을 제공합니다.



송신자(Proposer)가 개인키로 데이터에 서명 → 네트워크 전송 → 수신자(Validator)가 공개키로 서명 검증.

5.2 PQC 서명 메커니즘의 핵심 적용 범위 (Core Application of PQC Mechanism)

퀀타리움은 SPHINCS+ 계열의 구조를 선택적 옵션이 아닌, 네트워크 전반을 제어하는 기본 전자서명 메커니즘으로 채택했습니다. 이 보안 스택은 다음과 같은 네트워크 핵심 행위에 필수적으로 사용됩니다.

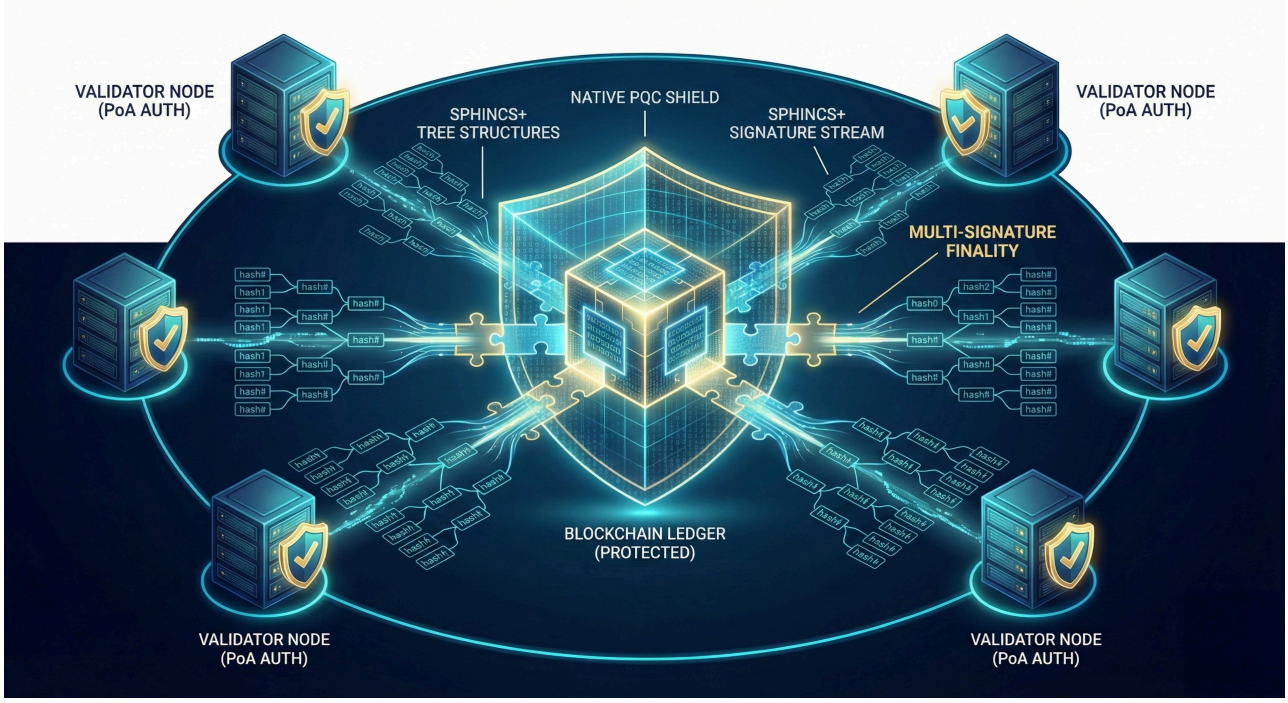
1. **트랜잭션의 생성 및 서명 (Transaction Integrity) :** 자산 전송 및 스마트 컨트랙트 호출 시, 사용자 개인키를 보호하고 거래의 무결성을 증명합니다.
2. **검증자(Validator)의 신원 인증 및 권한 증명 :** PoA 합의에 참여하는 노드의 정당성을 양자내성 암호로 인증하여, 네트워크 거버넌스에 대한 공격을 원천 차단합니다.
3. **합의 과정의 암호학적 증명 :** 블록 제안, 검증, 확정에 이르는 네트워크 참여 및 합의 프로세스 전반에서 발생하는 모든 서명 행위를 보호합니다.

5.3 계층별 통합 및 보안 영역의 명확화 (Layered Integration & Domain Definition)

퀀타리움의 PQC 보안 스택은 단일 지점에 머무르지 않고 **지갑(Wallet) 계층, 서명·검증(Sign/Verify) 계층, 합의 인증(Consensus Auth) 계층, 메시징 및 신원(Identity) 계층** 전반에 일관되게 적용됩니다.

특히 이 보안 스택은 시스템 아키텍처 내에서 **암호학적 보호 영역(Cryptographic Protection Domain)**과 **애플리케이션 로직 영역(Application Logic Domain)**을 명확히 분리하는 기준점이 됩니다.

- **투명한 책임 정의 :** 보안 스택은 핵심 암호 연산을 전담하고, 애플리케이션 로직은 비즈니스 프로세스만을 처리하도록 격리함으로써, 시스템의 보안 범위와 책임 한계를 투명하게 정의합니다. 이는 복잡한 dApp 로직의 오류가 메인넷의 보안 근간을 흔들지 못하게 하는 안전장치 역할을 수행합니다.



6. Layer 1 아키텍처 및 Proof of Authority(PoA) 합의

고성능 양자내성 합의 모델 (High-Performance PQC Consensus)

퀀타리움(Quantarium)은 타 블록체인에 종속된 토큰이나 사이드체인이 아닌, 독자적인 프로토콜과 원장을 보유한 **독립적인 Layer 1 블록체인**입니다. 우리는 양자내성 암호(PQC)가 필연적으로 수반하는 데이터 오버헤드를 시스템 레벨에서 수용하면서도, 엔터프라이즈급 서비스가 가능한 빠른 트랜잭션 처리와 예측 가능한 네트워크 성능을 보장하기 위해 **권한 증명(Proof of Authority, PoA)** 합의 방식을 채택했습니다.

6.1 독립적 Layer 1 인프라의 설계 목적 (Purpose of Independent Layer 1 Infrastructure)

기존의 EVM 기반 Layer 2 솔루션들은 확장성 문제를 해결할 수 있을지언정, 기저 레이어(Base Layer)인 이더리움 등이 가진 양자 취약성(ECDSA 의존성)을 상속받을 수밖에 없습니다.

- **네이티브 최적화 :** 퀀타리움은 독립적인 Layer 1 설계를 통해, SPHINCS+와 같은 대용량 서명 데이터를 효율적으로 처리할 수 있는 전용 블록 구조와 가스(Gas) 정책을 독자적으로 구현했습니다.
- **주권적 거버넌스 :** 외부 메인넷의 하드포크나 정책 변경에 휘둘리지 않고, NIST 표준 변경 등 암호학적 이슈에 즉각 대응할 수 있는 기술적 주권을 확보했습니다.

6.2 PoA 합의 메커니즘의 작동 원리 (Operational Mechanics of PoA Consensus)

퀀타리움의 PoA는 익명의 다수가 경쟁하는 것이 아니라, 검증된 소수의 노드가 협력하는 구조입니다.

- **연산 경쟁 제거 (No Mining Competition) :** PoW(작업 증명)와 달리 무의미한 해시 연산 경쟁을 완전히 제거했습니다. 이는 에너지 소비를 99% 이상 절감하며, 하드웨어 리소스를 오직 트랜잭션 검증과 스마트 컨트랙트 실행에만 집중시킵니다.
- **낮은 지연 시간과 높은 처리량 (Low Latency & High Throughput) :** 제한된 수의 검증 노드(Validator Nodes) 간에 최적화된 P2P 통신 경로를 형성하여 블록 전파 시간을 최소화했습니다. 이를 통해 수천 TPS 이상의 높은 처리량을 안정적으로 제공하며, 병목 현상 없는 실시간 결제 처리가 가능합니다.
- **예측 가능한 성능 :** 블록 생성 주기가 확률적이지 않고 결정론적(Deterministic)으로 유지되므로, 기업용 애플리케이션 운영에 필수적인 예측 가능한 네트워크 성능(SLA)을 보장합니다.

6.3 암호학적으로 검증된 권한 모델 (Cryptographically Verifiable Authority)

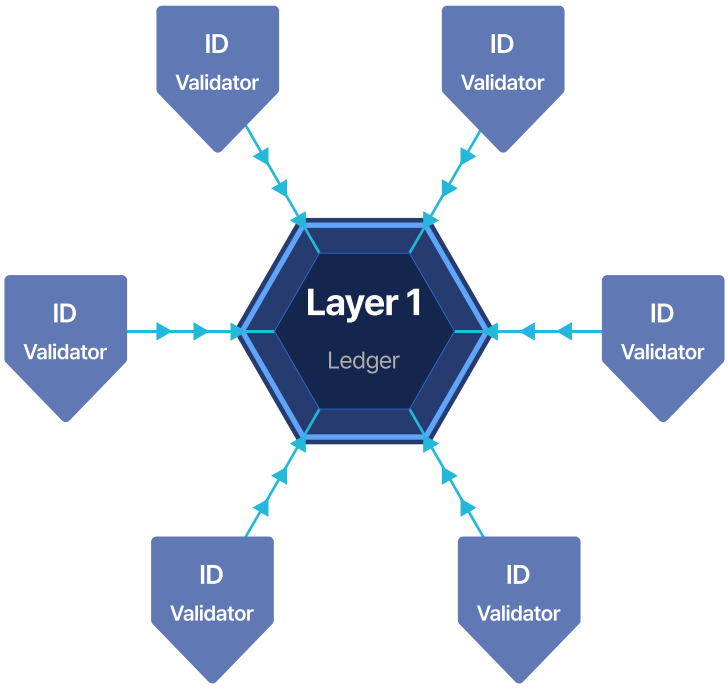
기존 PoA가 중앙화된 평판에만 의존했다면, 퀀타리움의 PoA는 PQC 기술과 결합된 신뢰 모델을 제시합니다.

- **QUANTA-X 및 SPHINCS+ 기반 신원 증명 :** 모든 검증 노드는 네트워크 참여 시 QUANTA-X 엔진을 통해 생성된 SPHINCS+ 키 쌍으로 자신의 신원을 증명해야 합니다. 이는 검증자의 권한(Authority)이 막연한 사회적 신용이 아닌, 수학적으로 검증 가능한 암호학적 서명(Digital Signature)에 기반함을 의미합니다.
- **검증 가능한 권한 위임 :** 합의 참여자의 신뢰성은 중앙 기관의 자의적 판단이 아닌, 스마트 컨트랙트에 명시된 거버넌스 규칙과 온체인 상의 암호학적 증거에 의해 투명하게 보장됩니다.
- **책임 추적성 (Accountability) :** 블록 생성자가 자신의 개인키로 블록에 서명(Signing)하므로, 악의적인 행위 발생 시 해당 노드를 즉각적으로 식별하고 배제(Slashing)할 수 있는 명확한 책임 소재를 제공합니다.

6.4 결론 : 실용주의와 보안의 균형

결론적으로 퀀타리움의 **Layer 1 PoA 아키텍처**는 양자내성이라는 '극한의 보안'과 상용 서비스가 요구하는 '쾌적한 속도'라는 두 마리 토끼를 잡기 위한 최적의 해답입니다. 우리는 암호학적으로 검증된 권한 모델을 통해, 탈중앙화의 이념을 훼손하지 않으면서도 현실 세계의 비즈니스를 수용할 수 있는 고효율 블록체인 환경을 제공합니다.

Quantarium PoA Consensus Architecture



7. PoA 거버넌스 및 검증자 운영 정책 (Governance & Validator Policy)

투명성과 책임성에 기반한 온체인 거버넌스

퀀타리움(Quantarium)의 거버넌스 모델은 탈중앙화된 네트워크의 유연성과 엔터프라이즈 환경이 요구하는 엄격한 통제력을 결합했습니다. 익명성에 기댄 무책임한 합의 참여를 배제하고, 수학적으로 검증된 신원과 명확한 프로토콜 규칙에 의거하여 네트워크를 운영합니다.

7.1 신뢰 기반의 진입 장벽: 검증자 자격 요건 (Validator Qualification)

퀀타리움 네트워크의 검증자(Validator)가 되기 위해서는 단순한 자본(Stake) 예치 이상의 엄격한 기술적, 법적 기준을 충족해야 합니다.

- **PQC 기반 암호학적 신원 바인딩 :** 예비 검증자는 QUANTA-X 엔진을 통해 생성된 SPHINCS+ 키 쌍을 네트워크에 등록해야 합니다. 이는 해당 노드의 운영 주체를 암호학적으로 특정하며, 향후 발생하는 모든 블록 생성 행위가 해당 주체의 서명에 의해 이루어짐을 보증합니다.
- **인프라 무결성 검증 :** 노드는 24/7 가용성(Availability)을 보장하는 고성능 하드웨어 스펙과 보안 모듈(HSM) 연동 환경을 갖추어야 하며, 이는 테스트넷 단계에서의 성능 벤치마크를 통해 사전 검증됩니다.
- **KYC/KYB 인증 :** 익명의 공격자가 네트워크를 장악하는 것을 방지하기 위해, 재단 또는 거버넌스 위원회를 통해 운영 주체의 실재성(법인 등)을 확인하는 절차를 거칩니다.

7.2 책임성 강화 메커니즘: 슬래싱 및 자동 퇴출 (Slashing & Automatic Revocation)

네트워크의 신뢰를 저해하는 행위에 대해서는 스마트 컨트랙트에 의해 즉각적이고 자동화된 제재가 가해집니다. 이를 통해 '선의'가 아닌 '시스템'에 의한 신뢰를 구축합니다.

- **이중 서명(Double Signing) 감지 :** 동일한 블록 높이에서 두 개 이상의 서로 다른 블록에 서명하는 행위는 포크(Fork)를 유발할 수 있는 중대한 공격입니다. SPHINCS+ 서명의 고유성을 이용해 이를 실시간으로 탐지하며, 적발 시 해당 노드의 권한은 즉시 정지됩니다.
- **가용성 미달(Downtime) :** 정해진 순서에 블록을 생성하지 못하거나 네트워크 동기화를 지연시키는 경우, 경고 누적 시스템(Reputation Score)에 의해 일시적으로 합의 그룹에서 제외되거나 자격이 박탈됩니다.
- **예치금 삭감(Slashing) :** 검증자가 예치한 보증금(Stake)은 악의적 행위가 증명될 경우 소각되거나 피해 보전 기금으로 전환됩니다. 이는 경제적 동기에 기반한 억지력을 제공합니다.

7.3 투명한 온체인 거버넌스 프로세스 (On-Chain Governance Process)

퀀타리움의 모든 정책 변경은 불투명한 회의실이 아닌, 블록체인 위에서 투명하게 결정됩니다.

- **제안 및 투표 (Proposal & Voting) :** 가스 비용(Gas Fee) 정책, 블록 크기 조정, PQC 파라미터 업데이트 등 네트워크의 주요 매개변수는 검증자 그룹의 투표를 통해 변경됩니다. 모든 투표 기록은 원장에 영구히 저장되어 감사가 가능합니다.
- **긴급 보안 프로토콜 :** 양자 컴퓨터 기술의 급격한 발전 등 긴급한 보안 위협이 감지될 경우, 전체 검증자의 2/3 이상 동의를 통해 즉시 보안 패치를 적용하거나 네트워크를 '비상 모드(Safe Mode)'로 전환할 수 있는 신속 대응 체계를 갖추고 있습니다.

7.4 규제 준수 및 감사 용이성 (Compliance & Auditability)

이러한 거버넌스 구조는 금융 기관 및 공공 부문이 블록체인을 도입할 때 직면하는 가장 큰 장벽인 '불확실성'을 제거합니다.

- **법적 책임 소재 명확화 :** 모든 트랜잭션과 블록은 신원이 확인된 검증자에 의해 처리되므로, 문제 발생 시 법적인 책임 소재를 명확히 할 수 있습니다.
- **실시간 감사 추적 :** 규제 당국이나 외부 감사인은 별도의 복잡한 절차 없이 블록체인 데이터를 조회함으로써 네트워크 운영 현황과 자금 흐름을 실시간으로 모니터링할 수 있습니다.

8. 양자내성 환경 스마트 컨트랙트 (Smart Contracts in PQC Environment)

실행 무결성과 접근 제어의 분리

퀀타리움(Quantarium)의 스마트 컨트랙트 아키텍처는 "언어의 복잡성"이 아닌 "실행의 안전성"에 초점을 맞춥니다. 우리는 양자내성(PQC) 기능이 컨트랙트 코드 문법 자체에 내재되어야 한다는 통념을 거부하며, 대신 접근 제어(Access Control)와 실행 로직(Execution Logic)을 명확히 분리하는 실용적인 접근 방식을 취합니다.

8.1 PQC의 적용 위치: 언어가 아닌 인증 계층
(PQC Location: Auth Layer, Not Language Syntax)

퀀타리움에서 스마트 컨트랙트를 작성하는 언어(Language) 자체에는 양자역학적 알고리즘이나 복잡한 암호 연산이 포함되지 않습니다. 이는 개발자의 진입 장벽을 낮추고 기존 개발 생태계를 포용하기 위함입니다.

- **서명 기반의 진입 장벽 :** 양자내성은 스마트 컨트랙트가 호출(Call)되는 시점, 즉 전자서명 및 인증 계층(Authentication Layer)에서 제공됩니다. 컨트랙트의 함수를 실행하려는 모든 트랜잭션은 반드시 SPHINCS+ 기반의 서명을 통과해야만 EVM(또는 실행 엔진) 내부로 진입할 수 있습니다.
- **로직과 보안의 분리 :** 개발자는 비즈니스 로직(DeFi, NFT 등) 구현에만 집중하며, 해당 로직을 누가 실행할 수 있는지에 대한 보안은 퀀타리움의 Core Layer가 PQC 서명을 통해 원천적으로 보증합니다.

8.2 보안 감사 용이성 (Ease of Security Auditing)

양자내성 구현을 위해 새롭고 난해한 프로그래밍 언어를 도입하는 것은 오히려 잠재적인 버그와 취약점을 증가시키는 위험 요소가 될 수 있습니다.

- **검증된 표준 준수 :** 퀀타리움은 업계 표준에 부합하는 스마트 컨트랙트 실행 환경을 제공하여, 기존의 보안 감사 도구(Audit Tools)와 형식 검증(Formal Verification) 방법론을 그대로 적용할 수 있도록 합니다.
- **코드 가독성 :** 스마트 컨트랙트 코드는 인간이 읽고 이해하기 쉬워야 합니다. 복잡한 암호학적 연산을 시스템 레벨로 추상화함으로써, 감사자(Auditor)는 로직의 결함에만 집중할 수 있어 감사의 효율성과 정확성을 높입니다.

8.3 실행 예측 가능성 (Execution Predictability)

엔터프라이즈 환경에서 스마트 컨트랙트는 결과가 결정론적(Deterministic)이어야 합니다.

- **격리된 샌드박스 :** 스마트 컨트랙트는 합의 엔진 및 PQC 암호 모듈과 완전히 격리된 샌드박스 환경에서 실행됩니다. 이는 특정 컨트랙트의 무한 루프나 오류가 네트워크 전체의 합의 프로세스에 영향을 주지 않도록 차단합니다.
- **가스 비용의 명확성 :** PQC 서명 검증 비용과 로직 실행 비용을 분리하여 산정함으로써, 사용자는 트랜잭션 실행에 필요한 비용을 사전에 정확하게 예측할 수 있습니다.

9. 퀀타리움 생태계 개요 (Ecosystem Overview)

통합된 양자내성 보안 루프 (Quantum-Resilient Security Loop)

퀀타리움 생태계는 개별 서비스의 단순한 집합이 아닙니다. 지갑(Wallet), 결제(Payment), 통신(Communication), 자산 이동(Asset Transfer)이라는 디지털 경제의 4대 요소가 하나의 끊어지지 않는 '양자내성 보안 루프' 안에서 유기적으로 통합된 구조입니다.

9.1 단일 PQC 보안 철학의 공유 (Shared PQC Security Philosophy)

생태계 내의 모든 애플리케이션(dApp)과 인프라는 **"처음부터 끝까지 안전하게(Secure from End-to-End)"**라는 동일한 보안 철학을 공유합니다.

- **보안의 통일성 :** 사용자가 지갑을 생성하는 순간부터, 메신저로 대화를 나누고, 자산을 전송하고, 결제를 완료하는 모든 과정에 **NIST 표준 SPHINCS+** 기반의 동일한 보안 강도가 적용됩니다. 이는 서비스 간 이동 시 보안 수준이 낮아지는 '약한 고리(Weak Link)'가 발생하지 않음을 의미합니다.
- **사용자 경험(UX)의 일관성 :** 복잡한 PQC 키 관리와 서명 과정은 백그라운드에서 처리되며, 사용자는 생태계 전반에서 일관되고 직관적인 인터페이스를 경험합니다.

9.2 생태계 핵심 구성 요소 (Core Ecosystem Components)

1. **Quantum-Resistant Wallet :** PQC 키 쌍의 안전한 생성과 보관을 담당하는 생태계의 관문입니다. 콜드 스토리지 지원 및 멀티 시그니처 기능을 통해 자산 탈취를 원천 봉쇄합니다.
2. **SECURET (Secure Communication) :** 단순한 메신저를 넘어, 지갑 주소와 연동된 암호화 통신 채널입니다. 양자 컴퓨터로도 해독 불가능한 메시지 전송을 통해 금융 정보 및 민감한 개인정보를 보호합니다.
3. **Asset Bridge :** 타 블록체인 자산을 퀀타리움 네트워크로 안전하게 가져오는 이동 통로입니다. 브릿지 과정에서도 PQC 검증을 수행하여 외부의 위협이 유입되는 것을 차단합니다.

9.3 구조적 격리와 확산 방지 (Structural Isolation & Containment)

퀀타리움 생태계는 고도로 연결되어 있지만, 동시에 보안적으로는 철저히 구획화(Compartmentalization)되어 있습니다.

- **취약성 확산 차단 :** 만약 생태계 내 특정 dApp이나 구성 요소에서 로직상의 취약점이 발견되더라도, 이것이 퀀타리움 메인넷의 합의 알고리즘이나 다른 자산의 보안으로 전이되지 않도록 설계되었습니다.
- **모듈형 보안 :** 각 구성 요소는 독립적인 보안 모듈을 통해 Core Layer와 통신하므로, 개별 서비스의 장애가 전체 시스템의 붕괴(Systemic Failure)로 이어지지 않는 견고한 회복 탄력성(Resilience)을 갖습니다.

10. 퀀타리움 이중 토큰 이코노미 (Quantarium Dual Token Economy)

10.1 개요 (Overview)

퀀타리움(Quantarium) 생태계는 기술적 안정성과 경제적 유동성을 동시에 확보하기 위해, 메인넷의 인프라 자산인 **QTA**와 거래소 생태계의 유틸리티 자산인 **QX**를 분리하여 운영하는 '이중 토큰 구조(Dual Token Structure)'를 채택했습니다. 이러한 설계는 메인넷의 보안 및 가스비 정책이 시장 변동성에 의해 위협받지 않도록 보호하는 동시에, 거래소 중심의 독자적인 경제 생태계가 유연하게 성장할 수 있는 기반을 제공합니다.

10.2 Quantarium 메인넷 코인 : QTA

(1) 정의 및 역할

QTA(Quantarium Coin)는 퀀타리움 양자내성 메인넷의 네이티브(Native) 자산입니다. 네트워크 내의 모든 트랜잭션 수수료(Gas Fee) 지불, 스마트 컨트랙트 실행, 그리고 검증자(Validator) 노드의 합의 참여를 위한 기본 통화로 사용됩니다.

(2) 발행 및 소각 모델 (Supply & Burn)

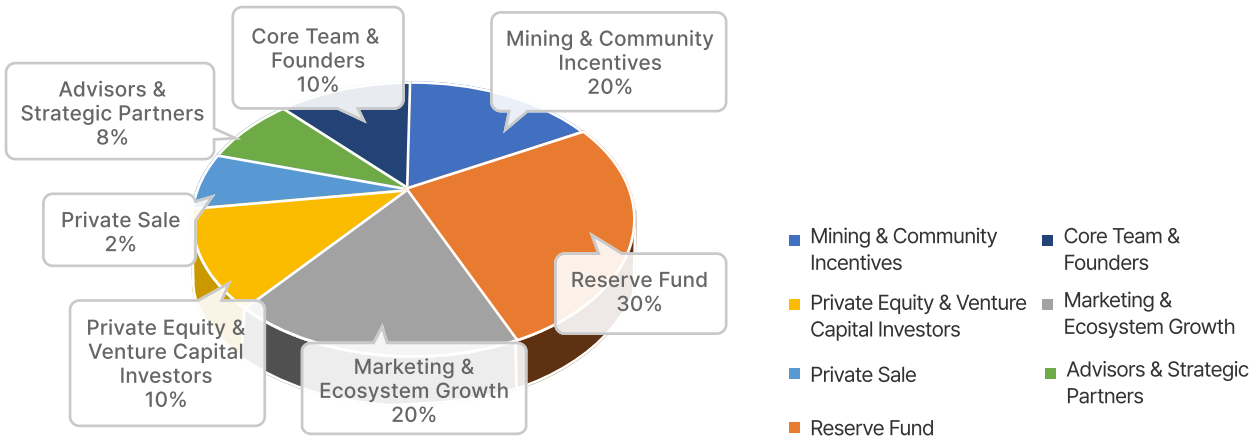
- **총 발행량 :** 1,000억 개 (100,000,000,000 QTA)
- **자동 소각 메커니즘 (Deflationary Model) :** QTA는 네트워크 사용량에 비례하여 가스비의 일정 부분이 자동으로 소각되는 알고리즘을 탑재하고 있습니다. 이는 생태계가 활성화될수록 유통량이 감소하여 코인의 희소 가치가 상승하는 디플레이션 구조를 형성합니다.

(3) QTA 초기 배분 구조 (Initial Allocation)

퀀타리움 재단은 장기적인 생태계 운영과 탈중앙화를 위해 다음과 같이 전략적으로 물량을 배분하였습니다.

Category (구분)	Allocation (%) (할당 비율)	수량 (Token Amount, QTA)	Description (설명)
Core Team & Founders (핵심 팀 및 창업자)	10%	10,000,000,000	QUANTARIUM 네트워크의 장기적 운영, 기술 유지보수 및 전략적 거버넌스를 위한 개발·창업 팀 보상으로 할당됩니다.
Advisors & Strategic Partners (어드바이저 및 전략 파트너)	8%	8,000,000,000	생태계 발전, 규제 준수, 글로벌 파트너십 확장을 지원하는 법률·기술·비즈니스 자문 그룹에 배분됩니다.
Marketing & Ecosystem Growth (마케팅 및 생태계 확장)	20%	20,000,000,000	사용자 확보, 글로벌 브랜딩, 커뮤니티 활성화 등 QUANTARIUM Coin의 채택과 생태계 확산을 위한 마케팅 활동에 사용됩니다.
Private Equity & Venture Capital Investors (사모 및 벤처 투자자)	10%	10,000,000,000	초기 단계에서 생태계 유동성 및 기술 확장을 지원하는 기관 및 전략적 투자자에게 배정됩니다.
Private Sale (프라이빗 세일)	2%	2,000,000,000	공인 투자자를 대상으로 한 제한적 사전 판매로, 초기 시장 형성과 프로젝트 자금 조달을 위한 비율입니다.
Mining & Community Incentives (채굴 및 커뮤니티 인센티브)	20%	20,000,000,000	채굴 보상, 스테이킹 프로그램, 사용자 참여 인센티브 등 탈중앙 검증과 생태계 기여를 촉진하기 위한 목적으로 사용됩니다.
Reserve Fund (예비/준비금)	30%	30,000,000,000	네트워크 안정성 유지, 연구개발(R&D) 자금, 전략적 파트너십 구축, 비상 유동성 확보 등을 위한 전략적 예비금으로 보유됩니다.
총 발행량 (Total Supply)	**100%**	**100,000,000,000**	

QTA 초기 배분 구조 (Initial Allocation)



QUANTARIUM 로드맵 (ROAD MAP)

2025

1 Quarter
양자 내성 알고리즘에 대한 타당성 조사 및 연구

2 Quarter
양자내성 알고리즘에 대한 기술이전계약 (ETRI)
양자내성 원본인증 기술 확보

3 Quarter
테스트넷 환경에서 프로토타입 블록체인 시스템 구현

4 Quarter
안정성 테스트를 거쳐 메인넷(실제 네트워크) 출시
암호화폐 지갑 핵심 기능 개발 및 연동
시큐릿메신저를 통한 지갑주소 연동(서버리스 보안구축)
시큐릿 메신저 안드로이드버전 1천만 다운로드 달성
시큐릿 메신저내 양자내성 암호화 구축 (쪽지,채팅)
동남아 파트너쉽 타진

2026

3 Quarter
자체 거래소 구축 및 QTA코인 상장 심의
NIST 표준 등 최신 양자 암호 기술 동향을 반영한 지속적인 업데이트
다른 블록체인 프로젝트 또는 기존 시스템과의 상호 운용성 확보
시큐릿 메신저 5천만 다운로드 달성
동남아 파트너십 확대 및 커뮤니티 활성화를 통한 생태계 확장

4 Quarter
QUANTARIUM 10대 거래소 상장

2027

1 Quarter
QUANTARIUM 양자내성 코인 전문 자체거래소 20위권 진출

2 Quarter
시큐릿메신저 1억다운로드 달성 및 자체거래소 10위권 진출

3 Quarter
QUANTARIUM 양자내성 자체거래소 글로벌거래소 3위권 진입

10.3 Quantarium Exchange 유틸리티 토큰 : QX

(1) 정의 및 특징

QX(Quantarium Exchange Token)는 퀀타리움 재단이 구축하는 자체 암호화폐 거래소(Quantarium Exchange)의 핵심 유틸리티 토큰입니다. QTA가 인프라 연료(Fuel)라면, QX는 서비스 참여 권한(Access)과 혜택을 부여하는 멤버십 토큰의 성격을 가집니다.

(2) 발행 및 유틸리티 (Supply & Utility)

- 총 발행량 : 10억 개 (1,000,000,000 QX) 추가 발행 없는 고정 수량
- 주요 유틸리티 :

A. 거래 수수료 할인 : QX 보유량에 따른 차등적 수수료 혜택 제공

B. 런치패드(Launchpad) 참여 : 유망 프로젝트의 초기 토큰 배정 우선권 부여

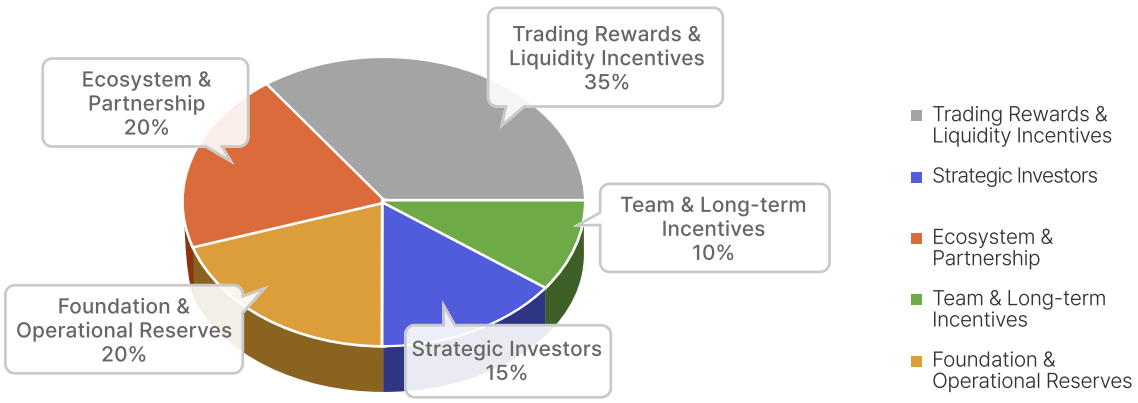
C. 거버넌스 투표 : 상장 심사 및 거래소 주요 정책에 대한 투표권 행사

D. PQC 보안 연동 : 사용자 지갑 간 이동 및 출금 시 메인넷의 PQC 전자서명을 적용하여 양자내성 보안 확보

(3) QX 유통 및 배분 구조 거래소 생태계의 유동성 공급과 참여자 보상에 중점을 둔 배분 정책을 시행합니다.

Category (구분)	Allocation (%) (할당 비율)	수량 (Token Amount, QX)	Description (설명)
Trading Rewards & Liquidity Incentives (거래 리워드 및 유동성 보상)	35%	350,000,000	유동성 공급과 거래 활성화를 위한 핵심 재원 거래 기여 보상, 유동성 공급자(LP) 인센티브, 스테이킹 보상
Ecosystem & Partnership (생태계 및 파트너십)	20%	200,000,000	글로벌 확장과 사용처 확대를 위한 전략적 예산 파트너십 확장, 마케팅 및 커뮤니티, 생태계 기금
Foundation & Operational Reserves (재단 및 운영 준비금)	20%	200,000,000	장기적인 생존과 안정적인 운영을 뒷받침하는 안전장치 운영 비용, 비상 예비비, R&D 투자
Strategic Investors (전략적 투자자)	15%	150,000,000	초기 자금 확보, 네트워크 활용
Team & Long-term Incentives (팀 및 장기 인센티브)	10%	100,000,000	핵심 인력의 동기 부여와 인재 영입
총 발행량 (Total Supply)	100%	1,000,000,000	

※ 모든 팀 및 투자자 물량에는 엄격한 베스팅(Vesting) 및 락업(Lock-up) 정책이 적용됩니다.



10.4 QTA와 QX의 상호보완적 시너지 (Structural Synergy)

QTA와 QX는 역할이 명확히 구분되면서도 상호 보완적으로 작동합니다. QTA의 가치는 메인넷 사용량(트랜잭션)에 비례하여 상승하며, QX의 가치는 거래소 플랫폼의 성장과 사용자 확대에 연동됩니다.

비교 항목	QTA (Mainnet Coin)	QX (Exchange Token)
성격	메인넷 네이티브 코인 (Infrastructure)	거래소 유틸리티 토큰 (Service)
총 발행량	1,000억 개 (100 Billion)	10억 개 (1 Billion)
주요 기능	가스비(Gas), 온체인 실행, 합의 검증	수수료 할인, 런치패드, 투표, VIP 혜택
가치 부양	자동 소각(Burn), 네트워크 수요 증가	유통량 감소(Lock-up), 플랫폼 수익 모델
보안 기술	Native PQC Layer 1 보호	출금/이동 시 PQC 서명 연동

10.5 시장 성장 잠재력 및 전망 (Market Potential Outlook)

퀀타리움 메인넷은 현존하는 블록체인들이 해결하지 못한 '양자 보안 위협'을 구조적으로 해결한 차세대 인프라입니다. 현재 블록체인 시장의 시가총액 규모와 양자 보안 기술의 수요 증가 추세를 고려할 때, 퀀타리움 생태계는 다음과 같은 성장 잠재력을 가집니다.

- 보안 프리미엄의 부상 : 2026년 이후 양자컴퓨터의 위협이 가시화됨에 따라, ECDSA 기반의 기존 메인넷에서 PQC 기반의 퀀타리움 메인넷으로 자산과 프로젝트가 이동하는 '디지털 마이그레이션' 수요가 급증할 것으로 전망됩니다.
- 시가총액 성장 시나리오 (Valuation Scenario) : 초기 생태계 안착 시의 보수적 전망부터, 글로벌 표준 메인넷으로 자리 잡는 낙관적 시나리오까지 단계적인 기업 가치 상승이 예상됩니다.

이러한 전망은 단순한 기대치가 아닌, 변화하는 글로벌 보안 표준(NIST 등)과 시장의 구조적 수요에 기반한 분석입니다.

11. 결론 (Conclusion)

양자 시대를 관통하는 불변의 신뢰 (Immutable Trust for the Quantum Era)

디지털 자산의 역사는 '신뢰'를 기술적으로 구현해 온 과정이었습니다. 그러나 다가오는 양자 컴퓨팅(Quantum Computing)의 파도는 기존 암호 체계(RSA, ECC)에 의존해 온 지난 수십 년간의 신뢰 구조를 근본적으로 위협하고 있습니다.

퀀타리움(Quantarium) 백서를 마무리하며, 우리는 기술적 지향점을 다시 한번 명확히 정의하고 미래를 향한 비전을 제시하고자 합니다.

10.1 퀀타리움의 정체성 : 오해와 진실(Identity of Quantarium: Clarification)

많은 이들이 '양자'라는 단어에서 오는 혼란을 겪습니다. 이에 퀀타리움은 우리의 기술적 본질을 다음과 같이 명확히 규정합니다.

> **"퀀타리움은 양자컴퓨터를 사용하는 블록체인이 아닙니다.""퀀타리움은 양자컴퓨팅 시대에도 살아남는 블록체인입니다."**

우리는 양자 역학적 현상(중첩, 얽힘)을 이용해 연산을 수행하는 하드웨어가 아닙니다. 퀀타리움은 양자 컴퓨터가 창과 같이 기존의 보안을 뚫고 들어올 때, 이를 막아낼 수 있는 유일한 방패인 '양자내성 암호(Post-Quantum Cryptography)'로 무장한 소프트웨어 프로토콜입니다. 우리는 공격 도구가 아니라, 인류의 디지털 자산을 지키는 방어 체계입니다.

10.2 불확실성을 넘어서는 구조적 회복력 (Structural Resilience Beyond Uncertainty)

'Harvest Now, Decrypt Later(지금 수집하고 나중에 해독한다)'는 공격 시나리오는 미래의 위협이 아닌 현재의 위기입니다. 퀀타리움은 이에 대응하기 위해 NIST 표준 SPHINCS+를 채택했습니다. 이는 특정 수학적 난제(소인수분해 등)의 붕괴에 영향을 받지 않는 해시 기반 구조를 통해, 양자 컴퓨터의 발전 속도나 알고리즘의 변화와 무관하게 시스템의 안전을 보장하는 구조적 회복력(Structural Resilience)을 확보했습니다.

10.3 실용주의적 혁신: 보안과 속도의 공존
(Pragmatic Innovation: Coexistence of Security and Speed)

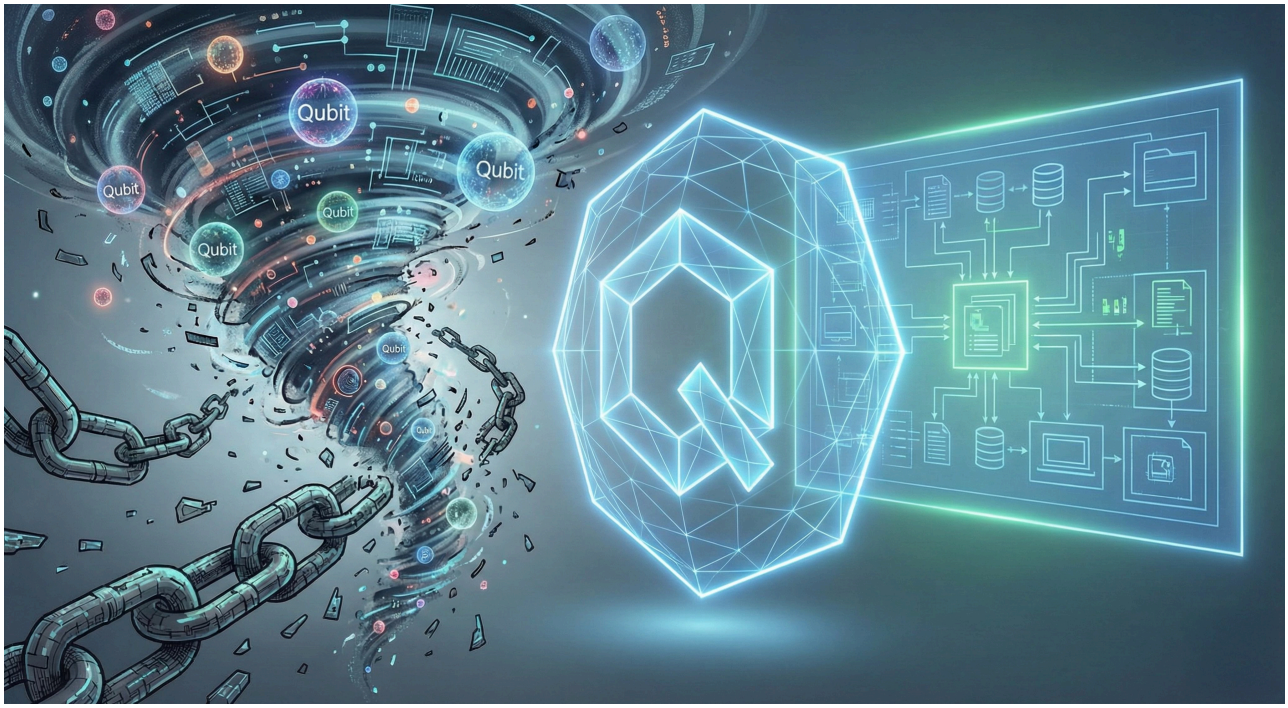
과거의 보안 강화 기술은 필연적으로 성능 저하를 동반했습니다. 그러나 퀀타리움은 **독립적인 Layer 1 아키텍처와 PoA(Proof of Authority)** 합의 알고리즘을 결합하여 이 딜레마를 해결했습니다. 암호학적으로 검증된 신뢰 노드를 통해 양자내성 암호의 무거운 연산 부하를 흡수하고, 엔터프라이즈 환경에서 요구하는 즉각적인 파이널리티(Instant Finality)와 **고속 트랜잭션**을 실현했습니다. 이는 퀀타리움이 이론적 실험실을 벗어나 현실 경제를 지탱할 준비가 되었음을 의미합니다.

10.4 맺음말 : 디지털 노아의 방주 (Closing: The Digital Noah's Ark)

기술의 발전은 축복이지만, 준비되지 않은 자에게는 재앙이 될 수 있습니다. 양자 우위(Quantum Supremacy)의 시대가 도래하여 기존 레거시 블록체인들의 방어막이 무너질 때, 퀀타리움은 가치를 안전하게 보존하고 미래로 전달하는 '디지털 노아의 방주'가 될 것입니다.

퀀타리움 생태계는 지갑, 결제, 통신, 자산 이동의 전 과정을 하나의 강력한 PQC 보안 루프로 통합했습니다. 이제 우리는 개발자, 기업, 그리고 모든 사용자에게 제안합니다. 가장 안전한 기반 위에서, 흔들리지 않는 미래를 함께 설계하십시오.

퀀타리움은 다가올 미래를 기다리지 않습니다. 우리는 그 미래를 견뎌낼 준비를 마쳤습니다.



12. 참고문헌 (References)

본 백서에 기술된 퀀타리움(Quantarium)의 보안 아키텍처, 양자내성 암호 표준, 그리고 합의 알고리즘은 다음의 국제 표준, 학술 논문 및 기술 보고서에 기반하여 설계되었습니다.

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.*
4. European Telecommunications Standards Institute (ETSI). *ETSI GR QSC 013: Quantum-Safe Cryptography; Threat Assessment.*
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.*