quantus

양자 보안, 암호화된 화폐

게시	버전	분류
2026년 3월 21일	0.3.3	public

본 백서는 정보 제공 목적으로만 제공되며, 어떠한 증권·투자 또는 금융 상품에 대한 매도 제안, 매수 제안의 권유 또는 권고를 구성하지 않습니다. 독자는 투자 결정을 내리기 전에 스스로 충분한 실사를 수행하고 자격을 갖춘 전문가와 상담해야 합니다. Quantus Network는 여기에 포함된 정보의 정확성이나 완전성에 대해 어떠한 진술이나 보증도 하지 않습니다.

목 차

01

서론

양자 위협

전통적인 블록체인은 암호학적으로 의미 있는 양자 컴퓨터(CRQC)로 인한 실존적 위협에 직면합니다. 블록체인의 암호학적 기반은 이산 로그 문제(DLP)의 난이도에 의존하며, 쇼어(Shor) 알고리즘을 포함한 양자 알고리즘은 DLP를 고전 컴퓨터보다 기하급수적으로 빠르게 풀 수 있습니다. 이러한 취약점은 양자 공격자가 공개 키에서 개인 키를 도출해 거래를 위조하고 민감한 금융 데이터를 복호화할 수 있게 할 수 있습니다.

> 선제적이고 양자 내성 컴퓨팅에 맞춘 업데이트가 없다면, 수조 달러 규모의 크립토 경제는 그러한 공격으로 인한 급격한 가치 하락 위험에 처합니다.

독특한 가치 제안

라틴어로 「얼마나」를 뜻하는 말에서 이름을 딴 Quantus Network는 확장 가능하고 양자 의미에서 안전한 사적 화폐(private money)를 가능하게 합니다. Quantus는 범용 스마트 컨트랙트 플랫폼이 아닙니다. 소수의 요리에 집중하는 레스토랑처럼, Quantus는 다음을 제공합니다.

- 모든 트랜잭션에 대한 포스트 퀀텀 서명

— 피어 간 연결을 보호하기 위한 포스트 퀀텀 서명 및 암호화(ML-DSA 및 ML-KEM)

— 확장을 위한 포스트 퀀텀 영지식 증명

— 도난을 억제하고 실수로부터 복구를 가능하게 하는 고보안 계정

— 주소를 간단히 검증할 수 있는 읽기 쉬운 확인 문구(check-phrases)

확장 가능하고 양자 의미에서 안전한 사적 화폐에 집중하기로 한 결정은 CRQC가 업계에 제기하는 위협과 비트코인이 이러한 과제를 다루지 못한다는 점에서 비롯됩니다.

02

블록체인에 대한 양자 위협

양자 컴퓨팅 기초

양자 컴퓨터는 중첩과 얽힘 같은 원리를 활용해 고전 기계로는 다루기 어려운 계산을 수행합니다. 0 또는 1인 고전 비트와 달리 큐비트는 동시에 여러 상태에 존재할 수 있어, 특정 문제에 대해 기하급수적 병렬성을 허용합니다. 이러한 능력은 블록체인 금융을 뒷받침하는 암호 시스템에 실존적 위험을 제기합니다. 양자 하드웨어용으로 개발된 알고리즘이 대부분의 공개 키 암호화 보안 가정을 무너뜨리기 때문입니다.

쇼어 알고리즘은 1994년 피터 쇼어(Peter Shor)가 제시한 것으로, 양자 컴퓨터에서 큰 정수의 인수분해와 이산 로그 문제를 다항 시간에 푸는 방법을 제공합니다. 양자 푸리에 변환(QFT)을 이용해 함수의 주기를 찾아 RSA나 타원곡선 암호(ECC) 등을 뒷받침하는 트랩도어 함수를 효율적으로 역전시킬 수 있습니다. 블록체인 금융 관점에서, 충분히 강력한 양자 컴퓨터(논리 큐비트 약 2,000개로 추정 [6][7][8][9])를 가진 공격자는 공개 키에서 개인 키를 다항 시간 $O(n^3)$에 도출할 수 있습니다. 이는 극단적인 가속으로, 취약한 시스템을 하룻밤 사이에 구식으로 만듭니다. [1]

그로버 알고리즘은 1996년 러브 그로버(Lov Grover)가 제안한 것으로, 비구조화된 검색에 대해 이차 가속을 제공해 검색 시간을 $O(n)$에서 $O(\sqrt{n})$ 연산으로 줄입니다. 비대칭 암호에 대한 쇼어만큼 파괴적이지는 않지만, 그로버는 해시 함수와 AES 암호화 같은 대칭 프리미티브에

영향을 미쳐 실질적으로 보안 수준을 절반으로 줄입니다(예: 256비트 키가 양자 공격에 대해 128비트처럼 동작). 이 공격은 암호 체계를 바꾸는 대신 보안 비트를 두 배로 늘리는 방식으로 완화됩니다. 또한 그로버의 이차 가속은 높은 큐비트·게이트 요구와 제한된 병렬화로 인해 수십억 번의 순차 연산이 필요해, 미래 하드웨어에서도 실제 역전에는 비현실적입니다. [2]

네 가지 위협 범주

01 - 디지털 서명 위조

쇼어 알고리즘은 대부분의 블록체인에서 사용하는 ECC 기반 서명(예: 비트코인의 secp256k1 곡선)을 직접 위협하여, 공격자가 사용자를 사칭하고 사기성 트랜잭션을 승인할 수 있게 합니다. 이러한 능력은 블록체인의 가장 기본적인 기능에 대한 치명적 실패를 의미합니다.

02 - 영지식 시스템에서 가짜 증명 위조

프라이버시 중심 금융을 위한 zk-SNARK 등 많은 영지식 증명은 커밋에 타원곡선 페어링을 통한 이산 로그 난이도에 의존합니다. 쇼어는 유효해 보이는 무효한 증명을 만들 수 있게 하여, 공격자가 새 코인을 발행하거나 레이어 2(L2) 상태를 위조할 수 있게 할 수 있습니다.

03 - 비밀 정보 복호화

양자 공격은 Zcash나 Monero 같은 프라이버시 프로토콜에서 취약한 공개 키 방식으로 보호된 암호화 데이터를 노출시킬 수 있습니다. 금융 프로토콜의 P2P 통신을 복호화해 민감한 자산 정보를 드러내고 표적 도난을 가능하게 할 수도 있습니다.

그로버 알고리즘은 작업 증명과 주소 생성에 쓰이는 SHA-256 등에 대한 원상(preimage) 공격을 가속할 수 있지만, 가장 덜 우려되는 위협입니다. 많은 포스트 퀀텀 암호 체계는 다이제스트가 충분히 크면 해시가 충분히 안전하다고 보는 해시 기반 구조를 포함합니다.

포스트 퀀텀 암호화의 확장 과제

포스트 퀀텀 암호화(PQC)는 양자 위협에 대한 필수적 보호를 제공하지만, 이러한 알고리즘의 고유한 설계로 인해 상당한 확장 장애물을 만듭니다. 콤팩트한 수학 구조에 의존하는 타원곡선 방식과 달리, PQC 프리미티브는 고전·양자 공격자 모두에 대한 보안을 유지하려면 더 큰 매개변수가 필요합니다. 그 결과 공개 키·개인 키·서명이 종종 수배~수십 배 커집니다. 아래 표는 128비트 포스트 퀀텀 보안 수준에서 ML-DSA의 전형적인 크기와 256비트 ECDSA 등 고전 대응물을 비교한 것입니다. [10]

알고리즘	공개 키	개인 키	서명
ML-DSA-87 (Dilithium)	**2,592 bytes**	**4,896 bytes**	**4,627 bytes**
ECDSA (256-bit)	**32 bytes**	**32 bytes**	**65 bytes**

128비트 포스트 퀀텀 보안 수준에서의 크기. 출처: Open Quantum Safe Project [10]

보시다시피 ML-DSA 서명은 ECDSA 대응물보다 70배 이상 클 수 있고, 공개 키는 80배 이상 클 수 있습니다. 다른 PQC 계열은 더합니다: SPHINCS+ 같은 해시 기반 방식은 최대 41KB의 서명을 낼 수 있고, 크기 최적화 격자 변형인 FALCON도 여전히 고전 크기를 상당한 배수로 초과합니다.

블록체인 맥락에서 이러한 팽창된 크기는 시스템적 확장 문제로 누적됩니다. 더 큰 서명은 개별 트랜잭션을 부풀려 블록이 더 빨리 차고 검증에 더 오래 걸리면서 초당 트랜잭션 수(TPS)를 낮춥니다. P2P 통신에도 부담을 주어 대역폭과 전파 지연이 늘고, 작업 증명 같은 합의에서 포크나 고아 블록 위험을 높일 수 있습니다. 저장 요구도 영향을 받아 노드 운영 비용이 오르고, 자원이 제한된 사용자나 검증자의 참여 장벽이 특히 커집니다.

> **참고**
>
> 이러한 확장 과제는 앞으로 모든 블록체인이 다뤄야 합니다. 예를 들어 비트코인은 최대 블록 크기를 늘리지 않으면 1 TPS도 훨씬 못 미칠 것입니다.

03

마이그레이션 위기

조정 문제

비트코인의 보수적 문화는 프로토콜 변경에 저항합니다. 어떤 PQC 개선도 마이그레이션 기한, 가능한 몰수, 블록 크기 증대 같은 논쟁적 이슈에 대한 합의를 요구합니다. 커뮤니티가 합의하더라도 각 사용자는 자산을 양자 안전 주소로 옮겨야 합니다. 마이그레이션은 모든 암호화폐 보유자의 행동을 요구하는데, 많은 이가 지갑 접근을 잃었거나 위협을 모릅니다.

이 문제는 모든 공개 블록체인에 있지만, 명확한 리더십 부재와 기술적 경화(osification) 철학 때문에 비트코인에 특히 어렵습니다.

분실 코인 문제

비트코인 중 약 2,500억~5,000억 달러가 분실된 키, 사망한 보유자, 잊힌 지갑 등으로 영구적으로 접근 불가능한 것으로 추정됩니다. [3] 이 코인은 마이그레이션할 수 없으며, 암호학적으로 의미 있는 양자 컴퓨터(CRQC)를 만드는 공적 보상처럼 작동합니다. 양자 공격자는 마이그레이션되지 않은 공개 키에서 개인 키를 도출해 수십억 달러 규모의 BTC를 시장에 쏟아낼 가능성이 큽니다.

> 유일한 기술적 해법은 마이그레이션되지 않은 코인을 동결하는 엄격한 기한을 두는 것인데, 이는 정치적으로 불가능합니다.

그런 기한 없이는 마이그레이션되지 않은 코인이 털리고 매도되어 시장이 붕괴하고 네트워크 신뢰가 무너질 것입니다.

마이그레이션 일정 문제

포스트 퀀텀 서명은 현재 비트코인 서명보다 20~80배 큽니다. 근본적인 아키텍처 변경 없이는 비트코인 성능이 이미 제한된 용량의 일부로 붕괴합니다.

비트코인이 정치·기술적 과제를 해결한다고 가정해도, 마이그레이션 자체는 수개월~~수년이 걸립니다. 각 보유자는 자금을 양자 안전 주소로 옮기기 위해 최소 한 번은 트랜잭션을 보내야 합니다. 많은 이가 먼저 시험 트랜잭션을 보낼 것입니다. 부풀려진 PQC 서명이 처리량을 질식시키면서, 네트워크는 취약한 코인이 여전히 노출된 채 수개월~~수년간 이어지는 대기열에 직면합니다.

> **QUANTUS의 대응**
>
> 이러한 누적 과제는 기존 체인에 양자 보안을 추가하는 일을 비현실적으로 어렵게 만듭니다. Quantus Network는 첫날부터 체인에 양자 보안을 통합해 이를 피합니다.

04

quantus network 아키텍처

기초

Quantus Network는 이더리움과 폴카닷 뒤의 팀인 Parity Technologies가 개발한 블록체인 SDK인 Substrate 위에 구축되어 있습니다. Substrate는 매우 모듈화되어 있어 Quantus만의 차별점에 집중하도록 구성 요소를 쉽게 교체할 수 있습니다.

Quantus는 Substrate를 다음과 같이 강화합니다.

- 포스트 퀀텀 서명 체계 지원 추가
- P2P 네트워크 보안을 포스트 퀀텀으로 업그레이드
- 사용자 제어 가능한 트랜잭션 가역성 추가
- 모든 데이터 타입을 필드 요소 한도에 맞춰 정렬해 데이터베이스를 ZK 친화적으로 구성

포스트 퀀텀 암호 프리미티브

Quantus Network는 NIST가 표준화한 PQC를 사용해 트랜잭션과 네트워크 통신이 양자 위협으로부터 안전하도록 합니다. 트랜잭션 무결성의 핵심은 **ML-DSA**(모듈-격자 기반 디지털 서명 알고리즘, 구 CRYSTALS-Dilithium)로, 보안·효율·구현 용이성의 균형으로 선택된 격자 기반 서명 방식입니다. ML-DSA는 모듈 격자상의 LWE(Learning With Errors)와 SIS(Short Integer Solution) 같은 문제의 난이도를 활

용해 쇼어 알고리즘을 포함한 고전·양자 공격에 강한 저항을 제공합니다. [4]

트랜잭션 서명을 위해 Quantus는 **ML-DSA-87**을 통합합니다. 이는 NIST 보안 레벨 5(고전 256비트·양자 128비트에 해당)로 가장 높은 매개변수 세트로, 격자 암호분석의 잠재적 진전에 대비합니다. 격자 암호는 상대적으로 새롭고 실전 검증이 고전 방식보다 덜했기 때문에 이 선택은 신중함을 우선합니다. 더 큰 매개변수는 격자 암호분석의 잠재적 진전 위험을 완화하며, 더 작은 키 크기가 여전히 더 약한 표적이 될 수 있습니다.

검토한 대안

ML-DSA는 FN-DSA(Falcon) 같은 대안보다 선택되었는데, FN-DSA는 구현 복잡도가 더 높습니다(예: 블록체인에 부적합한 부동소수점 연산 필요), 사양에 결정적 키 생성이 없으며, 개발 당시 비최종 상태였습니다.

SLH-DSA 같은 해시 기반 옵션은 서명이 더욱 커서(17KB 초과) 선택하지 않았습니다. 암호 민첩성(서명 체계 교체 능력)은 Substrate에 내장되어 있어, 향후 필요 시 이러한 대안을 비교적 쉽게 추가할 수 있습니다.

ML-DSA-87은 더 큰 키와 서명을 만들지만, Quantus 초기 단계 네트워크에서는 저장이 아직 병목이 아니어서 관리 가능하며, 영지식 증명을 통한 웜홀 주소 등 최적화가 확장을 다룰 것입니다.

구현 세부는 QIP-0006을 참고하세요.

libp2p - 양자 의미에서 안전한 네트워크

Quantus Network는 피어 투 피어(P2P) 노드 간 통신을 ML-DSA로 인증하고 **ML-KEM**(모듈-격자 기반 키 캡슐화 메커니즘, 구 CRYSTALS-Kyber)으로 암호화해 보호합니다. 이 통합은 libp2p 스택까지 PQC를 확장하며, 양자 내성을 위해 핵심 구성을 수정합니다: 피어 신원에는 ML-DSA-87 서명, 전송 보안에는 ML-KEM-768(양자 내성 공유 비밀을 위한 추가 KEM 메시지로 Noise 핸드셰이크 확장). [5]

P2P 레이어는 양자 보안 분석에서 종종 간과됩니다. 피어 인증은 중요하지만, 피어 수준에서 공격자가 할 수 있는 최악은 노드를 사칭하고 무효 메시지를 보내 서비스 거부를 일으키는 것입니다. 블록체인 모델에서 노드는 보통 신뢰되지 않으며 공격이 감지되면 키를 쉽게 바꿀 수 있어 이미 완화됩니다. P2P 통신 복호화도 공격자에게 이익이 제한적입니다(예: 트랜잭션 경로 추적은 프록시나 Tor로 완화), 대부분의 데이터는 결국 온체인에서 공개됩니다.

그럼에도 P2P 레이어를 양자 의미에서 안전하게 하면 도청, 중간자 공격, 양자 복호화로부터 보호되어 노드 가십, 블록 전파, 기타 네트워크 상호작용이 가까운 미래에도 기밀성과 무결성을 유지합니다.

기술 세부는 QIP-0004를 참고하세요.

pqc 확장 - 웜홀 주소

포스트 퀀텀 암호화에 내재된 확장 과제를 다루기 위해 Quantus Network는 **「웜홀 주소(Wormhole Addresses)」**라 불리는 혁신적인 집계형 포스트 퀀텀 서명 방식을 도입합니다. 이 시스템은 Plonky2 증명 시스템(기본적으로 STARK)로 생성한 영지식 증명(ZKP)

을 활용해 잔액 검증을 오프체인으로 옮겨, 체인이 개별 서명을 처리하지 않고 단일 컴팩트한 증명만 검증하게 합니다. 웜홀 주소는 하나의 증명으로 많은 트랜잭션을 검증할 수 있으며, 공개 입력(예: nullifier, 저장 루트, 출력 주소·금액)이 주된 제한 요인입니다. 이는 트랜잭션당 분할 저장 필요를 트랜잭션당 약 256바이트 추가 수준으로 줄여, 알려진 어떤 PQC 서명 방식보다 훨씬 작습니다.

이 방식의 양자 보안은 SNARK에서 흔한 양자 취약 타원곡선 페어링 대신, FRI(Fast Reed-Solomon Interactive Oracle Proofs)를 통한 커밋에 안전한 해시 함수 **Poseidon2**를 쓰는 데서 옵니다.

또한 인증 비밀은 Poseidon2 뒤에 숨겨집니다. 안전한 해시는 그로버에 의해 이차적으로만 약해지고 깨지지 않으므로, 해시 원상 증명은 SPHINCS+ 같은 해시 기반 방식과 유사하게 ZK 맥락에서 경량 포스트퀀텀 서명 역할을 할 수 있습니다.

클라이언트 / 증명자 흐름

사용자는 솔트와 비밀을 이어붙인 값을 이중 해시해 이중 지불이 불가능함이 증명 가능한 주소를 만듭니다.

```
H(H(salt|secret))
```

이 구조는 위양성(예: 단순 해시 공개 키를 소비 불가 주소와 혼동)을 막습니다. Substrate(및 일반적으로)에서 블록체인 주소는 안전한 해시가 아닌 대수 연산으로 개인 키에서 유도된 공개 키의 단순 해시이기 때문입니다. 구조의 보안은 안전한 해시의 이중 원상을 찾는 문제로 귀결됩니다. 이 주소로 보낸 토큰은 사실상 소각됩니다. 받은 주소에

대응하는 개인 키가 없어 지출할 수 없습니다. 이 코인은 공급을 늘리지 않고 재발행할 수 있습니다.

각 전송마다 전역 고유 전송 횟수 등의 세부가 담긴 TransferProof 저장 객체가 생성됩니다. 사용자 지갑은 최근 블록 헤더의 저장 루트에서 이 TransferProof 리프까지의 머클-패트리시아 트라이(MPT) 저장 증명을 생성합니다. 이중 지불을 막기 위해 nullifier를 계산합니다.

```
H(H(salt | secret | global_transfer_count))
```

집계자 흐름

누구나(클라이언트, 채굴자, 제3자) Plonky2 재귀로 여러 증명을 집계해 부모가 자식을 검증하는 증명 트리를 만들 수 있으며, 자식의 공개 입력을 집계합니다.

- nullifier는 그대로 전달
- 출력 주소는 중복 제거
- 블록 해시는 연결된 것으로 증명한 뒤 가장 최근 것만 남기고 폐기
- 중복 출력 주소의 금액은 합산

체인 / 검증자 흐름

네트워크는 집계 증명을 검증할 때 다음을 확인합니다: 블록 해시가 체인에 있고 최근인지, nullifier 고유성(이중 지불 방지), 증명 유효성. ZK 회로는 저장 증명의 정확성, nullifier 정확성, 주소의 소비 불가, 입출력 잔액 일치, 블록 헤더 연결을 강제합니다.

plonky2를 쓰는 이유

— 이미 감사됨

— 포스트 퀀텀

— 트러스티드 셋업 불필요

— 증명·검증 효율적

— 증명 집계가 자연스러움

— Rust 네이티브 구현

— Substrate의 no-std 환경과 호환

> **성능**
>
> 재귀 증명은 약 170밀리초에 끝나며 크기도 컴팩트합니다 (집계 증명당 약 100KB). 5MB 블록에 모든 트랜잭션이 동일 출력으로 가는 최적 경우, 웜홀 주소는 한 블록에 약 153,000건(nullifier당 32바이트로 4.9MB)을 담을 수 있어, 원시 ML-DSA 약 685건(5MB ÷ 7.3KB) 대비 약 223배 개선입니다.

보안 참고

잠재적 위험에는 회로·검증 구현 결함으로 인한 인플레이션 버그가 있으나, 재발행 코인이 영 지갑 주소 잔액을 초과하면 경제적으로 드러납니다. 사용자는 비밀을 공개하지 않고 첫 해시만 공개해 웜홀 주소임을 선택적으로 증명할 수 있습니다. 검증 트랜잭션은 서명되지 않으므로 실패 트랜잭션에 의한 DoS는 금융 수단 없이 완화해야 합니다.

토큰 공급 계산은 유지되는데, 재발행은 새 코인처럼 보이지만 소각을 통해 최대 공급 보장이 유지됩니다.

기술 세부는 QIP-0005를 참고하세요.

합의 메커니즘

Quantus Network는 작업 증명(PoW) 합의 알고리즘을 사용하며, 비트코인 합의의 바람직한 성질을 유지하면서 SHA-256을 **Poseidon2**로 바꿔 ZK 증명 시스템과의 호환성을 높입니다.

중요: 이 변경은 양자 보안 때문이 아닙니다. SHA-256 같은 암호학적 해시는 그로버 등 양자 알고리즘에 약해지지만 파괴되지는 않습니다. 일부 포스트 퀀텀 서명 방식은 이 이유로 안전한 해시를 기본 블록으로 씁니다.

Poseidon2는 Poseidon 해시의 개선입니다. SHA-256 같은 전통 해시로 SNARK·STARK를 만들면 Poseidon을 쓸 때보다 게이트가 거의 100배 많이 필요한 경우가 많습니다. Poseidon은 비트 연산이 아닌 필드 원소에 대한 대수 함수에 전적으로 의존합니다.

Poseidon2와 Plonky2에는 **골디락스(Goldilocks)** 필드를 사용합니다. 골디락스 필드의 차수는 부호 없는 64비트 정수에 들어가 효율을 높이면서도 견고함을 해치지 않습니다.

05

자산 보존

암호화폐 키를 다룰 때의 위험은 많지만 대부분 피할 수 있습니다.

가역 트랜잭션

Quantus Network는 사용자가 설정할 수 있는 가역 트랜잭션을 제공합니다. 발신자는 나가는 전송을 취소할 수 있는 시간 창을 둡니다. 이는 도난을 억제하고 실수를 바로잡으면서도 최종성을 희생하지 않습니다. 시스템은 타임스탬프가 있는 수정된 Substrate 「스케줄러」 팔렛을 사용합니다. 지갑은 발신자(취소 버튼 포함)와 수신자에게 카운트다운을 표시합니다.

가역 트랜잭션은 온체인 적용을 통해 탈중앙성을 유지하면서 새로운 보안 프로토콜을 가능하게 합니다.

기술 세부는 QIP-0009를 참고하세요.

확인 문구

Quantus Network는 블록체인 주소에 대한 읽기 쉽고 암호학적으로 안전한 체크섬인 「check-phrases」를 도입합니다. 주소를 해시해 BIP-39 단어 목록에서 짧고 기억하기 쉬운 단어 열을 만듭니다. 확인 문구는 오타, 변조, 주소 중독 공격으로부터 보호합니다. 50,000회 반복의 키 유도 함수로 레인보우 테이블 공격 비용을 높입니다. 큰 거래에서는 여전히 주소의 모든 문자를 확인해야 합니다.

기술 세부는 QIP-0008를 참고하세요.

고보안 계정

모든 계정은 나가는 모든 전송에 필수 가역 기간을 두는 「고보안 계정」으로 승격할 수 있습니다. 지정된 **가디언**(하드웨어 지갑, 멀티시그, 신뢰 제3자)은 가역 기간 동안 의심스러운 트랜잭션을 취소해 자금을 발신자·수신자 대신 가디언에게 보낼 수 있습니다. 이 옵트인 기능은 한 번 활성화되면 영구적이라 도둑이 끌 수 없습니다.

가디언은 연쇄될 수 있습니다: 고보안 계정의 가디언이 다시 고보안 계정이 되어 자체 가디언을 둘 수 있습니다. 이렇게 합성 가능한 계층이 생겨 각 가디언이 보호 대상 계정보다 상위 권한을 갖습니다. 설계는 합법적 전송의 최종성을 해치지 않으면서 사용자가 무단 활동을 발견하고 대응할 시간을 줍니다.

기술 세부는 QIP-0011를 참고하세요.

키 복구

많은 크립토 자산이 주인과 함께 묻혔습니다. Quantus Network는 고정 지연 후 언제든 자금을 인출할 수 있는 복구 주소를 간단히 지정하는 방법을 제공합니다. 그동안 소유자는 키에 접근할 수 있다면 복구를 거부할 수 있습니다. 이 기능은 생존을 가능하게 합니다: 법원이나 형식적 유산 없이 온체인 유언을 남길 수 있습니다.

hd-lattice

계층적 결정론적(HD) 지갑은 단일 시드 구문으로 모든 키를 백업해 수동 복사 대비 보안과 편의를 높이는 업계 표준입니다. Dilithium 같은 격자 방식에 맞추려면 두 가지 과제가 있습니다.

— HMAC-SHA512 출력이 특정 성질을 가진 환에서 샘플링한 다항식인 격자 개인 키를 직접 구성할 수 없습니다.

— 비강화 키 유도는 타원곡선 덧셈에 의존하는데, 격자에는 그에 해당하는 대수 연산이 없습니다(공개 키가 어떤 연산에도 닫혀 있지 않음).

Quantus Network는 첫 번째를 HMAC 출력을 키 자체가 아니라 개인 키를 결정적으로 구축하는 엔트로피로 쓰는 방식으로 다룹니다. 두 번째는 덜 치명적이며 격자 암호를 그에 맞게 조정할 수 있는지는 여전히 열린 연구 질문입니다.

기술 세부는 QIP-0002를 참고하세요.

06

토크노믹스와 거버넌스

Quantus Network는 변화하는 환경에 있으며 처음부터 모두 맞출 수 있다고 가정하지 않습니다. 그래서 단순한 출발점을 택하고 새 정보가 쌓이면 거버넌스가 시스템을 바꿀 수 있게 했습니다. 이 설계는 블록체인을 환경에 적응할 수 있는 살아 있는 실체로 만듭니다. 특히 Substrate 거버넌스 프로세스는 노드 운영자 간 최소한의 조정으로도 체인에 깊은 변경을 허용합니다.

블록 보상

Quantus Network는 비트코인을 본뜬 단순한 토크노믹스 모델을 씁니다. 최대 공급은 **2,100만 코인**이며, 간단한 휴리스틱이 블록 보상을 정합니다.

```
block_reward = (max_supply - current_supply) / co
```

이 휴리스틱은 current_supply에 block_reward가 더해지면서 완만히 감소하는 지수 곡선을 이루고, 다음 블록에서 계산되는 block_reward를 줄입니다. 수수료 소각 등으로 current_supply가 줄면 그만큼 블록 보상 예산에 반영됩니다. 상수는 소각이 전혀 없을 때 약 30년 안에 코인의 99%가 발행되도록 선택됩니다.

투자자 배분

Quantus Network는 자금을 넣으며 큰 위험을 감수한 투자자들의 도움으로 만들어졌습니다. 사모 투자자는 팀과 마찬가지로 4년 베스팅

일정이 적용됩니다. 공개 판매 투자자는 첫날부터 전액 유동성을 갖습니다. 공개 판매로 모은 자금은 토큰과 짝을 이루어 유동성(DEX, CEX, 마켓 메이커)에 사용됩니다. 이러한 투자자 배분과 유동성이 유일한 「프리마인」입니다. 나머지 토큰은 존재할 때까지 채굴로 나와야 합니다.

공개 판매 최대 10% 미만이 팔리면 유동성 토큰은 비례해 줄고, 나머지는 블록 보상으로 채굴자에게 발행됩니다.

회사 배분

새 기술을 성공 보장 없이 만들 위험을 감수한 팀에 보상하기 위해, 약 4년간 블록 보상의 일부가 회사로 갑니다. 이는 사실상 전체 공급의 약 **15%**에 해당하는 회사 베스팅 일정입니다.

그 시점 이후 회사 몫은 끄거나 조정하거나 토큰 보유자 표결에 따라 재지향할 수 있습니다.

트랜잭션 수수료

트랜잭션 유형	수수료 구조	귀속
표준	고정 수수료	채굴자
가역(고보안)	거래액의 1%	소각
ZK 집계	거래액의 0.1%	채굴자 50% / 소각 50%

포크 없는 업그레이드

Quantus Network는 Substrate 런타임 업그레이드를 통해 「포크 없는」 업그레이드를 지원합니다. 블록체인 핵심 로직(「런타임」)이 네트워크를 어지럽히거나 커뮤니티를 쪼개는 하드 포크 없이 진화할 수 있습니다. 온체인 거버넌스 국민투표로 승인된 제안이 런타임 스왑을 켜며 — 기존 WASM 코드 블롭을 한 블록에서 새 것으로 바꿔 — 상태 연속성과 운영을 보장합니다. 이 경로는 다운타임과 위험을 줄이고, 실제 사용이 개선점을 드러내며 프로토콜을 반복적으로 다듬을 수 있게 합니다.

커뮤니티가 시스템을 신뢰하게 되면 런타임 변경 권한은 악의적 행위자가 업데이트 과정을 장악할 경우 공격 표면을 줄이기 위해 크게 제한될 수 있습니다.

거버넌스 시스템

Quantus Network는 Substrate를 통해 폴카닷의 OpenGov 시스템을 이어받습니다. 토큰 보유자는 **신념 투표(conviction voting)**로 참여하며, 자산을 기간 동안 잠가 표결 가중치를 높입니다. 증폭은 1x(잠금 없음)부터 6x(최대 잠금)까지 가능합니다. 이 설계는 참여에 영향을 가격으로 묶어 장기 정렬을 장려합니다.

제안은 「오리진(origin)」이라 불리는 여러 투표 트랙으로 나뉩니다. 각 오리진은 맞춤 매개변수(예: 고영향 변경에는 초과 다수)와 스팸 방지 최소 예치금, 준비·집행 기간, 교착을 막는 결정 기한을 갖습니다. 이 다트랙 설계는 일상적 재정 지출부터 중요한 런타임 업그레이드까지 다양한 국민투표를 병렬로 처리합니다.

Technical Collective는 긴급 기술 사안을 제안·검토·화이트리스트하는 큐레이션 전문가 그룹으로, 전용 트랙으로 속도를 내고 커뮤니티 감시를 유지합니다.

Quantus는 이를 수정 없이 채택하되 초기에는 복잡도를 피하기 위해 미니멀 구성으로 시작합니다. 처음에는 Technical Collective 트랙만 활성화되어 프로토콜 업그레이드나 매개변수 조정 같은 고권한 결정에 쓰입니다.

이후 Quantus는 집행 불가능한 주제(기능 제안, 생태계 설문 등)에 대한 비구속적 커뮤니티 투표 트랙을 추가할 수 있습니다. 회사가 네트워크를 DAO에 넘기면 이 시스템은 구속력을 갖게 됩니다. 이런 단계적 접근은 초기에 사용자에게 불필요한 복잡도를 지우지 않으면서 향후 거버넌스 표결로 유기적으로 진화할 수 있게 합니다.

07

로드맵

2026년까지의 현재 로드맵이며 변경될 수 있습니다.

heisenberg inception 2024년 12월	자금 확보, Substrate 채택.
resonance alpha 2025년 7월	퍼블릭 테스트넷, Dilithium 서명, 가역 트랜잭션.
schrödinger beta 2025년 10월	기능 완비, 감사 준비.
dirac beta 2025년 11월	PoW를 Poseidon2로 전환, 감사 대응.
planck beta 2026년 1월	고보안 계정, 멀티시그, 하드웨어 지갑, ZK 통합.
bell mainnet 2026년 Q2	메인넷 출시.
fermi upgrade 2026년 Q4	ZK 증명 집계 인프라.

08

리스크

Quantus Network를 구축하는 데는 고유한 위험이 따릅니다.

구현 문제

설계가 아무리 좋아도 소프트웨어 로직 결함은 심각한 장애를 일으킬 수 있습니다.

nist 알고리즘 선택 문제

표준화 이후 ML-DSA, ML-KEM 등 선정된 포스트 퀀텀 표준에 결함이나 백도어가 드러날 수 있습니다. 최악의 경우 그런 결함으로 공개 키에서 개인 키를 도출해 서명을 위조할 수 있어 체인에 재앙적 고장 모드가 됩니다. 그런 결함이 공개되면 Quantus Network는 새 알고리즘으로 업그레이드할 수 있지만, 드물게 악용되면 영원히 발견되지 않을 수도 있습니다.

양자 컴퓨팅 일정

양자 진전이 예상보다 훨씬 늦어 PQC 필요 시점이 늦춰질 수 있고, 반대로 정부 등의 비밀 개발은 블록체인 커뮤니티가 빠르게 업데이트하지 못하면 갑작스러운 위협이 될 수 있습니다.

기타 고려

일반적인 채택 장벽, 금융·블록체인 규제 불확실성, 크립토 생태계 고유의 변동성.

09

참고문헌 및 추가 읽을거리

[1] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

[2] Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eight Annual ACM Symposium on Theory of Computing*, 212-219. https://doi.org/10.1145/237814.237866

[3] Chainalysis. (2024). *The Chainalysis 2024 Crypto Crime Report*. https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/

[4] National Institute of Standards and Technology. (2024). *FIPS 204: Module-Lattice-Based Digital Signature Standard (ML- DSA)*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

[5] National Institute of Standards and Technology. (2024). *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)*. U.S. Department of

Commerce. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

[6] Häner, T., Jaques, S., Naehrig, M., Roetteler, M., & Soeken, M. (2020). Improved quantum circuits for elliptic curve discrete logarithms. *arXiv:2002.12480*. https://arxiv.org/abs/2002.12480

[7] Gidney, C., & Ekerå, M. (2021). *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits*. *arXiv:1905.09749*. https://arxiv.org/abs/1905.09749

[8] Aggarwal, D., et al. (2021). Assessment of Quantum Threat To Bitcoin and Derived Cryptocurrencies. *ePrint IACR*. https://eprint.iacr.org/2021/967.pdf

[9] Roetteler, M., Naehrig, M., Svore, K. M., & Lauter, K. (2017). Quantum resource estimates for computing elliptic curve discrete logarithms. *arXiv:1706.06752*. https://arxiv.org/abs/1706.06752

[10] Open Quantum Safe Project. (n.d.). ML-DSA | Open Quantum Safe. Retrieved January 29, 2026, from https://openquantumsafe.org/liboqs/algorithms/sig/ml-dsa.html