Quantus Network Whitepaper

저자: Christopher Smith | **마지막 업데이트:** 2026년 1월 14일

서론

양자 위협

전통적인 블록체인은 양자 컴퓨팅의 등장으로 인해 실존적 위협에 직면해 있습니다. 블록체인의 암호학적 기반은 이산 로그 문제(DLP)의 난이도에 의존하지만, 쇼어(Shor) 알고리즘과 같은 양자 알고리즘은 고전 컴퓨터보다 기하급수적으로 빠르게 DLP를 해결할 수 있습니다. 이러한 취약점으로 인해 양자 공격자는 공개 키에서 개인 키를 도출할 수 있으며, 이는 거래 위조 및 민감한 금융 데이터 복호화로 이어질 수 있습니다.

그 결과는 치명적인 시스템 실패입니다. 선제적인 양자 내성 업그레이드가 없다면, 수조 달러 규모의 크립토 경제는 이러한 공격으로 인한 갑작스러운 가치 하락 위험에 처하게 됩니다.

> 💡 **TIP**
>
> **Quantus가 이를 해결합니다.**

독특한 가치 제안

라틴어로 "얼마나"를 뜻하는 단어에서 이름을 딴 Quantus Network는 확장 가능하고 양자 보안이 보장되는 부의 보존을 제공합니다. Quantus는 스마트 컨트랙트 플랫폼이 아닙니다. 대신, 메뉴가 없는 고급 레스토랑처럼 Quantus는 소수의 핵심 기능을 다른 어떤 chain보다 더 잘 수행하는 데 집중합니다.

구체적으로 Quantus는 다음을 사용합니다:

- 모든 거래에 대한 포스트 양자 signature
- 피어 연결을 보호하기 위한 포스트 양자 signature 및 암호화(ML-DSA 및 ML-KEM)
- 다른 블록체인과의 포스트 양자 Bridge 및 양자 보안 래핑 코인(wrapped coins) 생성
- 확장을 위한 포스트 양자 zero-knowledge-proofs
- 도난을 방지하고 실수로부터 복구를 가능하게 하는 고보안 계정
- 쉬운 주소 확인을 위한 사람이 읽을 수 있는 체크 구문(check-phrases)

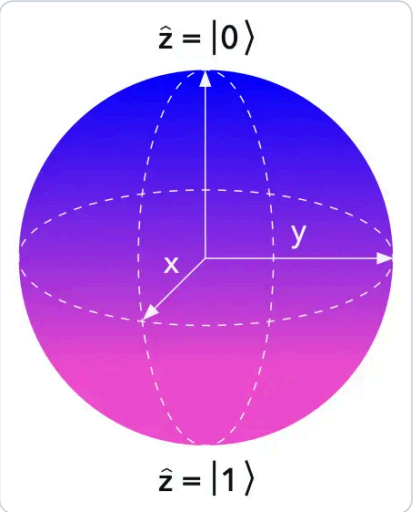
이러한 집중적인 접근 방식은 사용자가 자신 있게 부를 보존할 수 있도록 지원하며, 양자 위협을 기회로 바꿉니다.

> 💡 **TIP**
> Quantus는 미래를 대비한 당신의 자산을 위한 요새입니다.

블록체인에 대한 양자 위협

양자 컴퓨팅 기초

양자 컴퓨터는 중첩(superposition) 및 얽힘(entanglement)과 같은 원리를 활용하여 고전 컴퓨터로는 처리하기 힘든 계산을 수행합니다.



0 또는 1인 고전 비트와 달리, 양자 비트(qubit)는 동시에 여러 상태로 존재할 수 있어 특정 문제에 대해 기하급수적인 병렬 처리가 가능합니다. **이러한 능력은 블록체인 금융을 뒷받침하는 암호화 시스템에 실존적 위험을 초래합니다. 양자 하드웨어용으로 개발된 알고리즘이 대부분의 공개 키 암호화의 보안 가정을 무너뜨리기 때문입니다.**

쇼어 알고리즘(Shor's Algorithm)

1994년 피터 쇼어(Peter Shor)가 도입한 이 알고리즘은 양자 컴퓨터에서 큰 정수를 인수분해하고 이산 로그 문제를 다항식 시간 내에 해결하는 방법을 제공합니다. 본질적으로 양자 푸리에 변환(QFT)을 사용하여 함수의 주기를 찾아내며, RSA나 타원 곡선 암호(ECC)와 같은 방식의 기초가 되는 트랩도어 함수를 효율적으로 역전시킬 수 있게 합니다.

블록체인 금융의 관점에서, 이는 충분히 강력한 양자 컴퓨터(약 2,300개의 논리 큐비트로 추정)를 가진 공격자가 다항식 시간 $O(n^3)$ 내에 공개 키에서 개인 키를 도출할 수 있음을 의미합니다. 이는 극적인 속도 향상이며, 취약한 시스템을 하룻밤 사이에 쓸모없게 만듭니다.

그로버 알고리즘(Grover's Algorithm)

1996년 러브 그로버(Lov Grover)가 제안한 이 알고리즘은 비정형 검색 문제에 대해 이차 속도 향상(quadratic speedup)을 제공하여, 정렬되지 않은 데이터베이스에서 특정 항목을 찾는 시간을 O(n)에서 O(√n) 연산으로 단축합니다. 이는 양자 간섭을 통해 대상 상태의 진폭을 반복적으로 증폭함으로써 작동합니다. 비대칭 암호에 대한 쇼어 알고리즘만큼 파괴적이지는 않지만, **그로버 알고리즘은 해시 함수 및 AES 암호화와 같은 대칭 프리미티브에 영향을 미쳐 보안 수준을 사실상 절반으로 줄입니다** (예: 256비트 키가 양자 공격에 대해 128비트처럼 작동).

영향은 있지만, 이 공격은 암호화 방식을 바꾸는 것이 아니라 단순히 보안 비트를 두 배로 늘림으로써 완화될 수 있습니다. 또한 그로버의 이차 속도 향상은 높은 큐비트 및 게이트 요구 사항으로 인해 비실용적이며, 병렬화가 제한된 수십억 개의 순차 연산이 필요하므로 미래의 하드웨어에서도 실제 역전은 불가능에 가깝습니다.

양자 컴퓨팅이 블록체인 금융에 미치는 위험은 네 가지 영역으로 분류할 수 있습니다:

디지털 signature 위조

쇼어 알고리즘은 대부분의 블록체인에서 사용되는 ECC 기반 signature(예: 비트코인의 secp256k1 곡선)를 직접적으로 위협하여, 공격자가 사용자를 사칭하고 사기 거래를 승인할 수 있게 합니다. 이러한 능력은 블록체인의 가장 기본적인 기능의 치명적인 실패를 의미합니다.

제로 지식 시스템에서의 허위 증명 위조

프라이버시 중심 금융을 위한 zk-SNARKs와 같은 많은 제로 지식 증명은 커밋먼트를 위해 타원 곡선 페어링을 통한 이산 로그 난이도에 의존합니다. 쇼어 알고리즘은 유효해 보이는 유효하지 않은 증명을 생성할 수 있게 하여, 공격자가 새로운 코인을 발행하거나 레이어 2(L2)의 상태를 조작할 수 있게 할 수 있습니다.

비밀 정보 복호화

양자 공격은 Zcash나 Monero와 같은 프라이버시 프로토콜에서 취약한 공개 키 방식에 의해 보호되는 암호화된 데이터를 노출시킬 수 있습니다. 또한 금융 프로토콜의 p2p 통신을 복호화하여 민감한 자산 세부 정보를 드러내고 표적 도난을 가능하게 할 수 있습니다.

해시 함수 역전

그로버 알고리즘은 작업 증명 및 주소 생성에 사용되는 SHA-256과 같은 해시의 원상 공격(preimage attack)을 가속화할 수 있지만, 이는 가장 덜 우려되는 위협입니다. 많은 포스트 양자 암호화 방식은 해시가 충분히 큰 다이제스트를 가질 경우 충분히 안전하다고 간주되므로 해시 기반 구조를 통합합니다.

포스트 양자 암호화의 확장성 과제

포스트 양자 암호화(PQC)는 양자 위협에 대한 필수적인 보호를 제공하지만, 이러한 알고리즘의 고유한 설계로 인해 상당한 확장성 장애물을 도입합니다. 콤팩트한 수학적 구조에 의존하는 타원 곡선 방식과 달리, PQC 프리미티브는 고전 및 양자 공격자 모두에 대해 보안을 유지하기 위해 더 큰 매개변수를 필요로 합니다. 이로 인해 공개 키, 개인 키 및 signature가 종종 수십 배 더 커지게 됩니다.

다음 표는 128비트 포스트 양자 보안 수준에서의 ML-DSA의 일반적인 크기를 256비트 ECDSA와 같은 고전적 방식과 비교한 것입니다:

알고리즘	공개 키 크기 (바이트)	개인 키 크기 (바이트)	signature 크기 (바이트)
ML-DSA-87 (Dilithium)	2,592	4,896	4,627
ECDSA (256-bit)	32	32	65

표에서 볼 수 있듯이, ML-DSA signature는 ECDSA 대응물보다 70배 이상 클 수 있으며, 공개 키는 80배 이상 클 수 있습니다.

다른 PQC 제품군은 이를 더욱 악화시킵니다. SPHINCS+와 같은 해시 기반 방식은 최대 41KB의 signature를 생성할 수 있으며, FALCON과 같이 크기가 최적화된 격자 변형조차도 고전적 크기를 크게 초과합니다.

블록체인 맥락에서 이러한 팽창된 크기는 시스템적인 확장성 문제로 이어집니다. 더 큰 signature는 개별 거래를 비대하게 만들어, 블록이 더 빨리 채워지고 검증에 더 많은 시간이 필요함에 따라 초당 거래 수(TPS)를 감소시킵니다. 이는 또한 피어 투 피어(P2P) 통신에 부담을 주어 대역폭 요구 사항과 전파 지연을 증가시키며, 이는 작업 증명과 같은 합의 메커니즘에서 네트워크 포크나 고아 블록(orphan blocks)의 위험을 높일 수 있습니다. 저장 공간 요구 사항도 영향을 받아 노드 운영 비용이 상승하고, 특히 리소스가 제한된 사용자나 검증자의 참여 장벽이 높아집니다.

이러한 확장성 과제는 미래에 모든 블록체인이 해결해야 할 문제입니다. 예를 들어 비트코인은 최대 블록 크기를 늘리지 않는다면 1 TPS보다 훨씬 낮은 성능을 보이게 될 것입니다.

Quantus Network 아키텍처

포스트 양자 암호화 프리미티브

Quantus Network는 양자 위협으로부터 거래 및 네트워크 통신의 보안을 보장하기 위해 **NIST 표준 PQC** 프리미티브를 사용합니다. 거래 무결성의 핵심은 **ML-DSA(Module-Lattice-based Digital Signature Algorithm**, 이전 명칭 CRYSTALS-Dilithium)로, 보안, 효율성 및 구현 용이성의 균형을 위해 선택된 격자 기반 signature 방식입니다. **ML-DSA는 모듈 격자 상의 LWE(Learning With Errors) 및 SIS(Short Integer Solution)와 같은 문제의 난이도를 활용하여** 쇼어 알고리즘의 공격을 포함한 고전 및 양자 공격 모두에 대해 강력한 저항력을 제공합니다.

거래 signature를 위해 **Quantus는 ML-DSA-87을 통합합니다**. 이는 격자 문제의 잠재적인 암호 해독 돌파구로부터 보호하기 위해 최고 보안 수준(NIST 보안 레벨 5, 고전 256비트 및 양자 128비트 보안에 해당)을 제공하는 매개변수 세트입니다. 격자 암호화는 고전적 방식에 비해 상대적으로 새롭고 덜 검증되었기 때문에 이러한 선택은 신중함을 우선시합니다. 더 큰 매개변수는 격자 암호 해독의 잠재적 발전에 따른 위험을 완화하며, 더 작은 키 크기가 쉬운 표적이 될 때에도 안전을 유지합니다.

대안

ML-DSA가 FN-DSA(Falcon)와 같은 대안보다 선택된 이유는 다음과 같습니다:

- FN-DSA의 높은 구현 복잡성(예: 블록체인에 부적합한 부동 소수점 연산 필요)
- 사양에서 결정론적 키 생성의 부재
- 개발 당시의 비확정적 상태

SLH-DSA와 같은 해시 기반 옵션은 signature 크기가 훨씬 더 크기 때문에(17KB 초과) 거부되었습니다. Substrate에는 암호화 민첩성(다른 signature 방식을 교체할 수 있는 능력)이 내장되어 있어, 향후 필요에 따라 이러한 대안을 추가하는 것이 상대적으로 쉽습니다.

ML-DSA-87은 더 큰 키와 signature를 초래하지만, 이는 저장 공간이 아직 병목 현상이 아닌 Quantus의 초기 단계 네트워크에서 관리 가능하며, 제로 지식 증명을 통한 웜홀 주소(wormhole addresses)와 같은 향후 최적화가 확장성 문제를 해결할 것입니다.

구현에 대한 자세한 기술적 내용은 QIP-0006을 참조하십시오.

LibP2P

Quantus Network는 인증을 위한 ML-DSA와 암호화를 위한 ML-KEM(Module-Lattice-based Key Encapsulation Mechanism, 이전 명칭 CRYSTALS-Kyber)의 조합을 사용하여 피어 투 피어

(P2P) 노드 통신을 보호합니다.

이 통합은 PQC를 libp2p 네트워킹 스택으로 확장하여 양자 내성을 위해 핵심 구성 요소를 수정합니다. 구체적으로 피어 식별을 위해 ML-DSA-87 signature를 사용하고 전송 보안을 위해 ML-KEM-768을 사용합니다(양자 내성 공유 비밀을 위한 추가 KEM 메시지로 Noise 핸드셰이크 확장).

P2P 레이어는 양자 보안 분석에서 종종 간과됩니다. 피어 인증은 중요하지만, 피어 레벨에서 공격자가 할 수 있는 최악의 일은 노드를 사칭하고 유효하지 않은 메시지를 보내는 것이며, 이는 서비스 거부(DoS)로 이어질 수 있습니다. 이 공격은 블록체인 모델에서 노드가 일반적으로 신뢰되지 않는다는 점과 공격이 감지될 경우 노드가 키를 쉽게 바꿀 수 있다는 사실에 의해 이미 완화되었습니다. 마찬가지로 P2P 통신을 복호화하는 것은 공격자에게 제한된 이점만을 제공하며(예: 거래 경로 추적, 프록시나 Tor로 완화 가능), 대부분의 데이터는 어차피 온체인에서 공개됩니다.

그럼에도 불구하고 P2P 레이어를 양자 보안으로 보호하는 것은 도청, 중간자 공격 및 양자 복호화로부터 보호하여 노드 가십, 블록 전파 및 기타 네트워크 상호 작용이 예측 가능한 미래 동안 기밀로 유지되고 변조되지 않도록 보장합니다.

구현에 대한 자세한 기술적 내용은 QIP-0004를 참조하십시오.

PQC 확장성 확보

포스트 양자 암호화 고유의 확장성 과제를 해결하기 위해, **Quantus Network는 "웜홀 주소(Wormhole Addresses)"라고 불리는 혁신적인 집계형 포스트 양자 signature 방식을 도입합니다.** 이 시스템은 Plonky2 증명 시스템(기본적으로 STARKs)을 통해 생성된 제로 지식 증명(ZKPs)을 활용하여 잔액 검증을 오프체인으로 이동시켜, 체인이 개별 signature를 처리하지 않고도 단일 압축 증명을 검증할 수 있게 합니다.

웜홀 주소는 하나의 증명으로 대량의 거래를 검증할 수 있게 하며, 공개 입력(예: nullifiers, 저장 루트, 출구 주소 및 금액)이 주요 제한 요인이 됩니다. 이는 거래당 분할된 저장 공간 수요를 **거래당 약 256바이트 추가 수준으로 줄이며, 이는 알려진 어떤 PQC signature 방식보다 훨씬 작습니다.**

이 방식의 양자 보안은 SNARKs에서 흔히 사용되는 양자 취약 타원 곡선 페어링 대신, FRI(Fast Reed-Solomon Interactive Oracle Proofs)를 통한 커밋먼트에 안전한 해시 함수 Poseidon2를 사용하는 데서 비롯됩니다.

또한 인증 비밀은 Poseidon2 뒤에 숨겨져 있습니다. 안전한 해시 함수는 그로버 알고리즘에 의해 이차적으로만 약화될 뿐 무너지지 않으므로, 해시 원상 증명은 SPHINCS+와 같은 해시 기반 방식과 유사하게 ZK 컨텍스트에서 경량 포스트 양자 signature 역할을 할 수 있습니다.

클라이언트 / 증명자(Prover) 흐름

사용자는 솔트(salt)와 비밀(secret)을 결합한 값을 이중 해시하여 증명 가능하게 소비 불가능한 주소를 생성합니다:

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

이 구조는 위양성(예: 단일 해시 공개 키를 소비 불가능한 주소로 오해하는 것)을 방지합니다. Substrate(및 일반적으로)에서 블록체인 주소는 공개 키의 단일 해시이며, 공개 키는 안전한 해시가 아닌 대수적 연산을 통해 개인 키에서 도출되기 때문입니다. 따라서 이 구조의 보안은 안전한 해시의 '원상의 원상'을 찾는 것으로 귀결됩니다. 이 주소로 전송된 토큰은 사실상 소각(burn)됩니다. 해당 주소에 대한 개인 키가 존재하지 않으므로 소비할 수 없기 때문입니다. 따라서 이러한 코인은 공급량을 늘리지 않고도 다시 발행(re-mint)될 수 있습니다.

각 전송에 대해 고유한 글로벌 전송 횟수와 같은 세부 정보를 포함하는 TransferProof 저장 객체가 생성됩니다. 사용자의 지갑은 최근 블록 헤더의 저장 루트에서 이 TransferProof 리프까지의 MPT(Merkle-Patricia-Trie) 저장 증명을 생성합니다.

Nullifier가 계산됩니다:

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

비밀은 보존을 위해 지갑 시드에서 결정론적으로 도출되어 이중 지출을 방지합니다.

집계자(Aggregator) 흐름

어떤 당사자(클라이언트, 채굴자 또는 제3자)든 Plonky2의 재귀를 사용하여 여러 증명을 집계하여 증명 트리를 형성할 수 있습니다. 여기서 각 부모 증명은 자식 증명의 검증이며, 자식 증명의 공개 입력이 집계됩니다:

- nullifiers는 변경 없이 전달됨
- 출구 주소는 중복 제거됨
- 블록 해시는 연결된 것으로 증명된 후 가장 최근의 것을 제외하고 모두 삭제됨
- 중복된 출구 주소의 금액은 합산됨 이러한 재귀는 계층적 집계를 지원하여 온체인 데이터를 획기적으로 줄입니다.

체인 / 검증자(Verifier) 흐름

네트워크는 다음을 확인하여 집계된 증명을 검증합니다:

- 블록 해시가 온체인에 있고 최신인지 여부

- nullifier의 고유성(이중 지출 방지)
- 증명의 유효성

ZK 회로는 다음을 강제합니다:

- 저장 증명의 정확성
- nullifier 계산의 정확성
- 주소의 소비 불가능성
- 입력과 출력 간의 잔액 일치
- 블록 헤더 연결

Plonky2가 선택된 이유는 다음과 같습니다:

- 이미 감사됨
- 포스트 양자 보안
- 신뢰할 수 있는 설정(trusted setup) 불필요
- 효율적인 증명/검증
- 원활한 증명 집계
- Rust 네이티브 구현
- Substrate의 no-std 환경과 호환

성능 하이라이트:

170밀리초 이내의 재귀 증명 및 압축된 크기(집계된 증명당 100KB)로 엄청난 처리량 향상을 가능하게 합니다.

5MB 블록과 모든 거래가 동일한 출력으로 향하는 최적의 경우, **원홀 주소는 단일 블록에 약 153,000건의 거래를 담을 수 있습니다** (4.9MB / nullifier당 32바이트). 이는 약 685건의 원시 ML-DSA 거래(5MB / 각 7.3KB)보다 223배 향상된 수치입니다.

보안 참고 사항

잠재적 위험에는 잘못된 회로/검증 구현으로 인한 인플레이션 버그가 포함되지만, 이는 다시 발행된 코인이 제로 전송 주소의 잔액을 초과할 경우 경제적으로 감지 가능합니다. 사용자는 선택적으로 비밀을 밝히지 않고 첫 번째 해시를 게시하여 주소가 원홀임을 증명할 수 있습니다. 검증 거래는 서명되지 않으므로, 실패한 거래를 통한 서비스 거부는 비금융적으로 완화되어야 합니다. 토큰 공급량 계산은 유지됩니다. 다시 발행된 코인은 새 코인으로 나타나지만 소각을 통해 최대 공급량 보장이 유지되기 때문입니다.

구현에 대한 더 자세한 기술적 내용은 QIP-0005를 참조하십시오.

합의 메커니즘

Quantus Network는 비트코인 합의 알고리즘의 바람직한 특성을 유지하면서 SHA-256을 Poseidon2로 교체하여 ZK 증명 시스템과의 호환성을 향상시킨 작업 증명(PoW) 합의 알고리즘을 사용합니다.

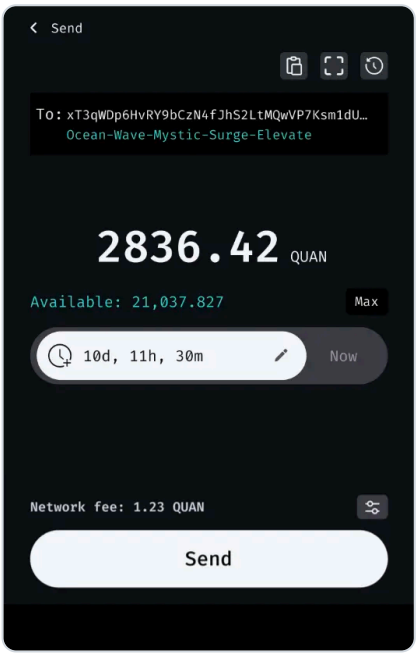
중요한 점은, 이 변경이 양자 보안을 위해 이루어진 것이 아니라는 것입니다. SHA-256과 같은 암호화 해시 함수는 그로버 알고리즘과 같은 양자 알고리즘에 의해 약화되지만 파괴되지는 않습니다. 이러한 이유로 일부 포스트 양자 signature 방식은 안전한 해시를 빌딩 블록으로 사용합니다.

Poseidon2는 Poseidon 해시 함수의 개선판입니다. SHA-256과 같은 전통적인 해시 함수를 포함하는 계산에 대해 SNARKs 또는 STARKs를 생성하는 것은 비트 수준 연산 대신 필드 요소 상의 대수 함수에만 의존하는 Poseidon을 사용하는 것보다 거의 100배 더 많은 게이트가 필요합니다. 효율성을 극대화하기 위해 Poseidon2와 Plonky2 모두에 Goldilocks 필드를 사용합니다.

부의 보존

암호화폐 키 관리에는 많은 위험이 따릅니다. 그 중 대부분은 피할 수 있습니다. Quantus Network는 체인 자체에 사용 편의성을 내장하여 전문가가 아닌 사람도 안심하고 거래할 수 있도록 합니다.

취소 가능한 거래(Reversible Transactions)

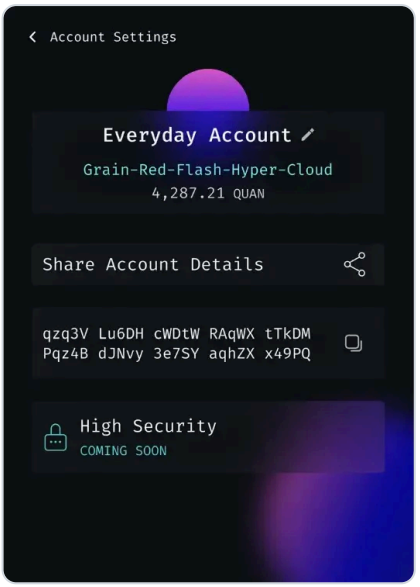


Quantus Network는 사용자 설정이 가능한 취소 가능한 거래를 제공하여, 송금인이 보낸 송금을 취소할 수 있는 시간 창을 설정할 수 있게 함으로써 블록체인의 핵심인 불가역성을 훼손하지 않으면서 도난 방지 및 오류 수정을 강화합니다. 직관적인 지연을 위해 타임스탬프를 사용하는 수정된 Substrate "스케줄러 팔레트(scheduler pallet)"를 활용하여, 시스템은 간단한 인터페이스를 통해 송금을 예약할 수 있게 하며, 지갑에는 송금인(취소 버튼 포함)과 수신인(취소되지 않을 경우 완료됨을 표시) 모두를 위해 카운트다운이 표시됩니다. 이는 상거래를 위한 빠른 최종성과 실수를 걱정하거나 에스크로 서비스 없이 신의 성실 예치금을 내고 싶어하는 사용자를 위한 유연성 사이의 균형을 맞춥니다.

취소 가능한 거래는 온체인 강제를 통해 탈중앙화를 유지하면서 새로운 보안 프로토콜을 위한 강력한 빌딩 블록을 형성합니다.

자세한 기술적 내용은 QIP-0009를 참조하십시오.

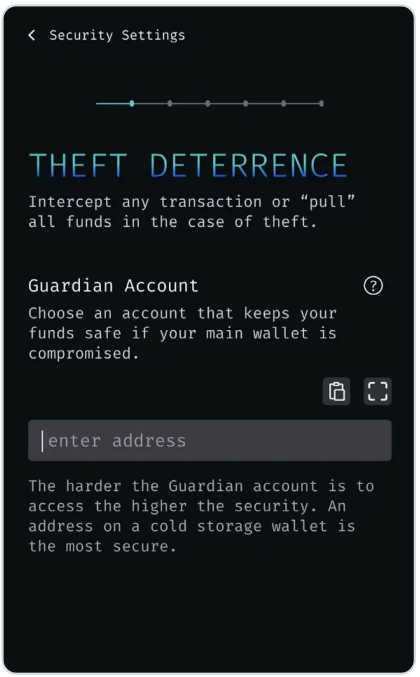
체크 구문(Check-Phrases)



Quantus Network는 블록체인 주소 및 기타 사람의 확인이 필요한 데이터를 위해 암호화되어 안전하고 사람이 읽을 수 있는 체크섬인 "체크 구문(check-phrases)"을 도입합니다. **주소를 해시하여 BIP-39 니모닉 리스트에서 기억하기 쉬운 짧은 단어 시퀀스를 생성함으로써, 체크 구문은 빠르고 오류 없는 무결성 확인을 가능하게 하여 오타, 변조 및 주소 포이즈닝(address poisoning)과 같은 공격으로부터 보호합니다.** 이 도구는 사용자가 잘린 표시나 취약한 체크섬에 의존하지 않고 송금 중에 자신 있게 주소를 확인할 수 있게 합니다. 특정 체크섬에 대한 레인보우 테이블 생성을 매우 비싸게 만들기 위해 50,000회 반복 키 도출 함수가 사용됩니다. 물론 고액 거래의 경우 사용자는 여전히 주소의 모든 글자를 수동으로 확인하여 정확성을 점검해야 합니다.

자세한 기술적 내용은 QIP-0008을 참조하십시오.

고보안 계정



Quantus Network는 모든 계정을 "고보안 계정"으로 업그레이드할 수 있는 기능을 제공합니다. 이 계정은 모든 송금에 대해 의무적인 취소 기간을 강제하며, 하드웨어 지갑, 멀티시그 또는 사용자가 선택한 신뢰할 수 있는 제3자와 같은 지정된 "가디언(guardian)" 계정이 취소 기간 동안 의심스러운 거래를 독점적으로 취소할 수 있게 합니다. 취소된 자금은 송금인이나 수신인이 아닌 가디언에게 전송됩니다. 이 선택적 영구 기능은 취소 가능한 송금을 기반으로 구축되었으며, 사용자는 활성화 시 지연 시간과 차단기(interceptor)를 지정하여 도둑이 이를 비활성화하는 것을 방지합니다.

차단기 자체도 자체 가디언을 가진 또 다른 고보안 계정이 될 수 있어, 각 가디언이 보호하는 계정에 대해 상위 권한을 갖는 조합 가능한 계층 구조를 가능하게 합니다. 이 디자인은 전통적인 금융의 법원 명령 취소를 모방하지만 사용자 제어가 가능합니다. 이는 고액 계정에 대해 보안과 편의성의 균형을 맞추며, 정당한 흐름에 대한 블록체인 최종성을 저해하지 않으면서 승인되지 않은 활동을 감지하고 대응할 수 있는 시간을 제공합니다.

자세한 기술적 내용은 QIP-0011를 참조하십시오.

키 복구

많은 크립토 자산이 소유자와 함께 무덤으로 사라졌습니다. Quantus Network는 고정된 지연 시간을 조건으로 언제든지 자금을 인출할 수 있는 복구 주소를 지정하는 간단한 방법을 제공합니다. 이 기간 동안 소유자는 키에 접근할 수 있는 경우 복구를 거부할 수 있습니다. 이 기능은 생존성을 가능하게 합니다. 사용자는 법원이나 유산 관리 없이도 온체인 유언장을 가질 수 있습니다.

HD-Lattice

계층적 결정론적(HD) 지갑은 블록체인의 산업 표준으로, 사용자가 모든 키에 대해 하나의 시드 구문을 백업할 수 있게 하여 작업당 수동 백업보다 보안과 편의성을 향상시킵니다.

이를 Dilithium과 같은 격자 방식에 적응시키는 데는 두 가지 과제가 있습니다:

- HMAC-SHA512 출력은 격자 개인 키를 직접 형성할 수 없으며, 거부 샘플링(rejection sampling)을 통한 "양호한 기저" 다항식이 필요합니다.
- 비경화(non-hardened) 키 도출은 타원 곡선 가산에 의존하지만 격자에는 이것이 없습니다 (공개 키는 어떤 대수적 연산에 대해서도 닫혀 있지 않음).

Quantus Network는 HMAC의 출력을 개인 키 자체가 아니라 개인 키를 결정론적으로 구성하기 위한 엔트로피로 사용하여 첫 번째 문제를 해결합니다. 두 번째 문제는 덜 중요하며 격자 암호화가 이를 해결하기 위해 적응될 수 있는지 여부는 여전히 열린 연구 과제로 남아 있습니다.

자세한 기술적 내용은 QIP-0002를 참조하십시오.

토크노믹스 및 거버넌스

Quantus Network는 변화하는 환경 속에 존재하며, 첫 번째 시도에서 모든 것을 완벽하게 해낼 것이라고 가정할 수 없습니다. 이러한 이유로 우리는 간단한 시작점을 선택하고 새로운 정보가 습득됨에 따라 거버넌스 시스템이 변경을 수행할 수 있도록 합니다. 이 디자인은 블록체인을 환경에 마음대로 적응할 수 있는 살아있는 실체로 만듭니다. 특히 Substrate 거버넌스 프로세스는 다양한 노드 운영자 간의 최소한의 조정으로 체인에 깊은 변경을 가능하게 합니다.

블록 보상

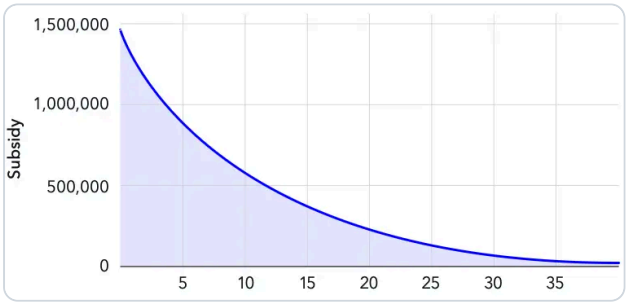
Quantus Network는 비트코인을 모방한 직접적인 토크노믹스 모델을 사용합니다. 최대 공급량은 21,000,000개이며 간단한 휴리스틱이 각 블록의 보상을 결정합니다.

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

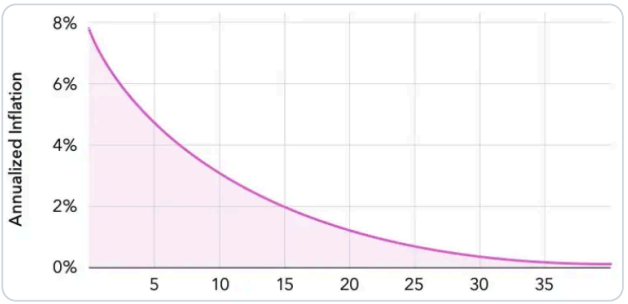
이 휴리스틱은 블록 보상이 현재 공급량(current_supply)에 기여하고 이것이 다음 블록에서 계산되는 블록 보상을 감소시키기 때문에 매끄러운 지수 쇠퇴 곡선을 형성합니다.

수수료 등으로 인한 모든 소각은 현재 공급량을 감소시키며 본질적으로 블록 보상을 위한 예산의 일부가 됩니다. 상수는 소각이 없을 때 약 40년 후에 코인의 99%가 발행되도록 선택됩니다.

연간 블록 보상



연간 인플레이션



투자자 할당

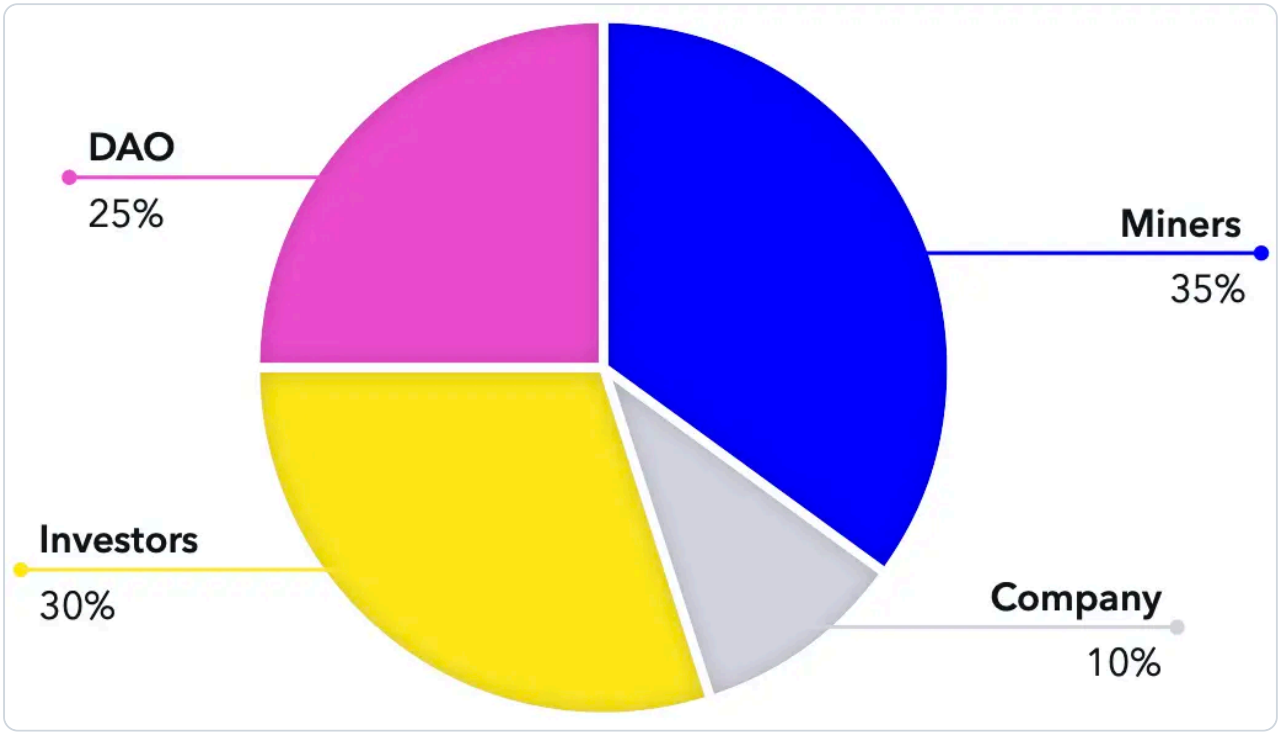
Quantus Network는 자금을 지원하며 큰 위험을 감수한 엔젤 투자자들의 도움으로 구축되었습니다. 투자자 락업(lockups)이 생성하는 공급 오버행을 피하기 위해, 우리는 공공 및 민간을 포함한 모든 투자자가 첫날부터 유동성을 가질 수 있도록 합니다. 이 할당은 유일한 "사전 채굴(pre-mine)"이 될 것입니다. 다른 모든 토큰은 채굴을 통해 존재해야 합니다. 공모 판매의 성공 여부에 따라 이 부분은 총 공급량의 20-30%를 차지하게 됩니다.

회사 할당

성공 보장 없이 새로운 기술을 구축하는 위험을 감수한 팀에 보상하기 위해, 우리는 블록 보상을 두 부분으로 나눕니다. 첫 번째 절반은 채굴자에게 돌아갑니다. 약 4년 동안 두 번째 절반은 회사에게 돌아갑니다. 이는 회사에게 총 공급량의 약 10%에 해당하는 사실상의 베스팅(vesting) 일정을 제공합니다. 이 기간 동안 채굴자들은 새로 발행된 코인을 동일한 양만큼 받게 됩니다.

그 시점 이후 회사의 블록 보상 부분은 토큰 보유자가 관리하는 금고(treasury)로 리디렉션되어 사실상 DAO를 형성하게 됩니다.

대략적인 공급 할당



거래 수수료

표준 거래에는 채굴자에게 돌아가는 수수료가 있어 거래를 포함할 인센티브를 제공합니다. 고보안 계정에서의 취소된 거래에는 거래량 기반 1% 수수료가 부과되며, 이는 절반은 채굴자에게 돌아가고 절반은 소각되어 미래 보안 예산으로 들어갑니다. zk 집계 시스템을 통과하는 거래에도 거래량 기반 0.1% 수수료가 부과되며, 이는 채굴자, 증명 집계자 및 소각 간에 분할됩니다.

포크리스 업그레이드(Forkless Upgrades)

Quantus Network는 Substrate의 런타임 업그레이드를 통해 "포크리스" 업그레이드를 지원하여, 네트워크를 중단시키거나 커뮤니티를 분열시킬 수 있는 하드 포크 없이 블록체인의 핵심 로직("런타임")을 진화시킬 수 있게 합니다. 이는 온체인 거버넌스 국민투표를 통해 달성되며, 승인된 제안은 런타임 교체를 트리거하여 본질적으로 단일 블록 내에서 기존 WASM 코드 블롭을 새

블롭으로 교체함으로써 상태와 운영의 연속성을 보장합니다. 이러한 업그레이드 경로는 다운타임과 위험을 최소화하여 커뮤니티가 프로토콜을 반복적으로 개선할 수 있도록 지원합니다.

거버넌스 시스템

Quantus Network는 Substrate를 통해 Polkadot의 OpenGov 시스템에서 거버넌스 프레임워크를 상속합니다. 토큰 보유자는 확신 투표(conviction voting)를 통해 참여하며, 투표의 무게를 증폭시키기 위해 다양한 기간 동안 자산을 잠그는 데 동의합니다. 이러한 증폭은 1배(잠금 없음)에서 6배(최대 잠금)까지 가능합니다. 이 디자인은 영향력을 약속에 연결함으로써 장기적인 일치를 장려합니다.

제안은 "오리진(origins)"이라고 불리는 여러 투표 트랙으로 분류됩니다. 각 오리진은 승인 임계값(예: 영향이 큰 변경의 경우 절대 다수), 스팸 방지를 위한 최소 보증금, 준비/시행 기간 및 교착 상태 방지를 위한 결정 시간라인과 같은 맞춤형 매개변수를 가집니다. 이러한 다중 트랙 디자인은 일상적인 금고 지출부터 중요한 런타임 업그레이드에 이르기까지 다양한 국민투표의 병렬 처리를 가능하게 합니다.

기술 위원회(Technical Collective)는 긴급한 기술 문제를 제안, 검토 또는 화이트리스트에 추가하는 전문 기관 역할을 하는 엄선된 기술 전문가 그룹으로, 커뮤니티 감독을 유지하면서 전용 트랙을 통해 신속하게 처리합니다.

Quantus는 수정 없이 이 시스템을 채택하지만 초기 단계의 복잡성을 피하기 위해 최소한의 설정으로 시작합니다. 초기에는 기술 위원회 트랙만 활성화되며, 이는 프로토콜 업그레이드나 매개변수 조정과 같은 구속력 있는 고권한 결정에 사용됩니다.

나중에 우리는 기능 제안이나 생태계 설문 조사와 같은 비구속적 주제에 대한 여론을 측정하기 위한 비구속적 커뮤니티 투표 트랙을 도입할 것입니다. 이 시스템은 회사가 네트워크를 DAO로 넘길 때 구속력을 갖게 될 것입니다.

이러한 단계적 접근 방식은 시작할 때 사용자에게 불필요한 복잡성을 부담시키지 않으면서 향후 거버넌스 투표를 통해 네트워크가 유기적으로 진화할 수 있게 합니다.

로드맵

Heisenberg Inception

2024년 12월

자금 확보, **Substrate** 선정

Resonance Alpha

2025년 7월

공개 테스트넷, **Dilithium** 서명, 취소 가능한 거래

Schrödinger Beta

2025년 10월

기능 완성, 감사 준비 완료

Dirac Beta

2025년 11월

PoW를 **Poseidon2**로 변경, 감사 사항 대응

Planck Beta

2026년 1월

고보안 계정, 멀티시그, 하드웨어 지갑

Bell Mainnet

2026년 1분기

메인넷 런칭

Fermi Upgrade

2026년 2분기

ZK 집계

위험

Quantus Network를 구축하는 데는 내재된 위험이 따릅니다.

- **구현 문제:** 소프트웨어 로직의 결함은 아무리 잘 설계된 시스템에서도 심각한 실패를 초래할 수 있습니다.
- **NIST 알고리즘 선택 문제:** 선택된 포스트 양자 표준(예: ML-DSA, ML-KEM)에서 표준화 이후 나타날 수 있는 잠재적 결함이나 백도어. 최악의 경우, 이러한 결함은 공격자가 공개 키에서 개인 키를 도출하여 signature를 위조할 수 있게 하여 체인의 치명적인 실패 모드를 나타낼 수 있습니다. 이러한 결함이 공개되면 Quantus Network는 새 알고리즘으로 업그레이드될 수 있지만, 이러한 결함이 은밀하게 이용된다면 결코 발견되지 않을 수도 있습니다.
- **양자 컴퓨팅 시간라인:** 양자 돌파구가 예상보다 훨씬 늦게 도착하여 PQC의 필요성이 지연될 수 있습니다. 반대로, 정부 등에 의한 비밀스러운 개발은 블록체인 커뮤니티가 신속하게 업데이트하지 못할 경우 갑작스러운 위협으로 이어질 수 있습니다.
- **기타 고려 사항:** 일반적인 채택 장벽, 금융/블록체인 분야의 규제 불확실성, 크립토 생태계 고유의 변동성.

맺음말

QUANTUS

우리는 오픈 프로토콜, 작업 증명, 그리고 주권적 소유권의 힘을 믿습니다. 데스크톱과 모바일에서 사용 가능한 Quantus Network 앱을 통해 사용자는 디지털 자산을 저장하고, 새로운 블록을 채굴하며, 중개자 없는 더 공정한 금융 미래에 참여할 수 있습니다.

우리는 투명성, 프라이버시, 그리고 안전한 셀프 커스토디얼(self-custodial) 도구를 통해 개인의 역량을 강화하는 데 전념하고 있습니다.