Quantus Network Whitepaper

Autoren: Christopher Smith | **Zuletzt aktualisiert:** 14. Januar 2026

Einleitung

Die Quantenbedrohung

Traditionelle Blockchains stehen vor einer existenziellen Bedrohung durch das Aufkommen des Quantencomputings. Die kryptografischen Grundlagen von Blockchains beruhen auf der Schwierigkeit des diskreten Logarithmusproblems (DLP). Quantenalgorithmen, insbesondere der Shor-Algorithmus, können das DLP exponentiell schneller lösen als klassische Computer. Diese Schwachstelle könnte es Quanten-Angreifern ermöglichen, private Schlüssel aus öffentlichen Schlüsseln abzuleiten, was es ihnen erlauben würde, Transaktionen zu fälschen und sensible Finanzdaten zu entschlüsseln.

Das Ergebnis wäre ein katastrophaler Systemausfall. Ohne proaktive quantenresistente Upgrades riskiert die Billionen-Dollar-Kryptoökonomie eine plötzliche Abwertung durch solche Angriffe.

> 💡 **TIP**
>
> **Quantus löst dies.**

Einzigartiges Wertversprechen

Benannt nach dem lateinischen Wort für „wie viel", bietet Quantus Network skalierbare, quantensichere Vermögenserhaltung. Quantus ist keine Smart-Contract-Plattform. Stattdessen konzentriert sich Quantus, wie ein High-End-Restaurant ohne Speisekarte, darauf, eine kleine Anzahl von Dingen besser zu machen als jede andere chain.

Konkret nutzt Quantus:

- Post-Quanten-signature für alle Transaktionen
- Post-Quanten-signature und Verschlüsselung (ML-DSA und ML-KEM) zur Sicherung von Peer-Verbindungen

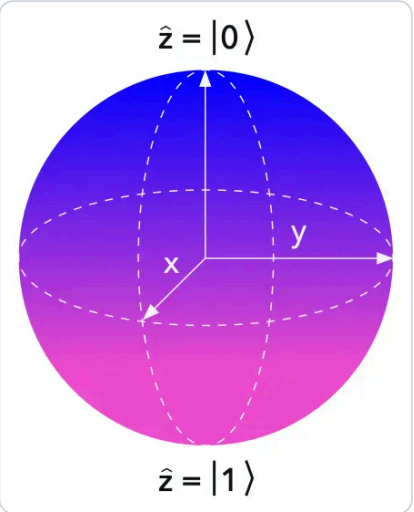
- Eine Post-Quanten-Bridge zu anderen Blockchains und die Erstellung quantensicherer Wrapped Coins
- Post-Quanten-zero-knowledge-proofs zur Skalierung
- Hochsicherheitskonten zur Abschreckung von Diebstahl und zur Ermöglichung der Wiederherstellung nach Fehlern
- Für Menschen lesbare check-phrases zur einfachen Adressverifizierung

Dieser gezielte Ansatz ermöglicht es Nutzern, ihr Vermögen vertrauensvoll zu bewahren und Quantenbedrohungen in Chancen zu verwandeln.

> 💡 **TIP**
> Quantus ist die zukunftssichere Festung für Ihr Vermögen.

Die Quantenbedrohung für die Blockchain

Grundlagen des Quantencomputings



Quantencomputer nutzen Prinzipien wie Superposition und Verschränkung (Entanglement), um Berechnungen durchzuführen, die für klassische Maschinen unlösbar sind.

Im Gegensatz zu klassischen Bits, die entweder 0 oder 1 sind, können Quantenbits (Qubits) gleichzeitig in mehreren Zuständen existieren, was einen exponentiellen Parallelismus für bestimmte Probleme ermöglicht. **Diese Fähigkeit stellt existenzielle Risiken für die kryptografischen Systeme dar, die die Blockchain-Finanzierung unterstützen, da für Quantenhardware entwickelte Algorithmen die Sicherheitsannahmen der meisten Public-Key-Kryptografien untergraben.**

Shor-Algorithmus

Der 1994 von Peter Shor eingeführte Algorithmus bietet eine Methode in Polynomialzeit zur Faktorisierung großer ganzer Zahlen und zur Lösung des diskreten Logarithmusproblems auf einem Quantencomputer. Im Wesentlichen nutzt er Quanten-Fourier-Transformationen (QFT), um die Periode einer Funktion zu finden, was eine effiziente Umkehrung der Trapdoor-Funktionen ermöglicht, die Schemata wie RSA oder Elliptic Curve Cryptography (ECC) zugrunde liegen.

Für die Blockchain-Finanzierung bedeutet dies, dass ein Angreifer mit einem ausreichend leistungsstarken Quantencomputer (geschätzt auf ~2.300 logische Qubits) private Schlüssel aus öffentlichen Schlüsseln in Polynomialzeit $O(n^3)$ ableiten könnte. Dies ist eine extreme Beschleunigung, die anfällige Systeme über Nacht obsolet macht.

Grover-Algorithmus

Der 1996 von Lov Grover vorgeschlagene Algorithmus bietet eine quadratische Beschleunigung für unstrukturierte Suchprobleme und reduziert die Zeit zum Finden eines bestimmten Elements in einer unsortierten Datenbank von $O(n)$ auf $O(\sqrt{n})$ Operationen. Er funktioniert durch iterative Verstärkung der Amplitude des Zielzustands

durch Quanteninterferenz. Obwohl er für die asymmetrische Kryptografie nicht so verheerend ist wie der Shor-Algorithmus, **beeinflusst Grover symmetrische Primitive wie Hash-Funktionen und AES-Verschlüsselung, wodurch das Sicherheitsniveau effektiv halbiert wird** (z. B. verhält sich ein 256-Bit-Schlüssel bei Quantenangriffen wie 128 Bit).

Obwohl wirkungsvoll, wird dieser Angriff durch einfaches Verdoppeln der Sicherheitsbits gemildert, anstatt das kryptografische Schema zu ändern. Darüber hinaus ist Grovers quadratische Beschleunigung aufgrund der hohen Anforderungen an Qubits und Gatter unpraktisch, da sie Milliarden von Operationen in Folge erfordert, bei begrenzter Parallelisierung, was eine Umkehrung in der realen Welt selbst auf zukünftiger Hardware undurchführbar macht.

Die Gefahren des Quantencomputings für die Blockchain-Finanzierung lassen sich in vier Bereiche unterteilen:

Fälschen digitaler signature

Der Shor-Algorithmus bedroht direkt ECC-basierte signature, die in den meisten Blockchains verwendet werden (z. B. Bitcoins secp256k1-Kurve), und ermöglicht es Angreifern, sich als Nutzer auszugeben und betrügerische Transaktionen zu autorisieren. Eine solche Fähigkeit würde ein kritisches Versagen der grundlegendsten Funktion einer Blockchain darstellen.

Fälschen falscher Beweise in Zero-Knowledge-Systemen

Viele Zero-Knowledge-Beweise, wie sie in zk-SNARKs für privatsphärorientierte Finanzen verwendet werden, beruhen auf der Schwierigkeit des diskreten Logarithmus über Elliptic-Curve-Pairings für Commitments. Der Shor-Algorithmus könnte die Erstellung ungültiger Beweise ermöglichen, die gültig erscheinen, was es einem Angreifer erlauben könnte, neue Coins zu prägen oder den Zustand von Layer-2s (L2s) zu fälschen.

Entschlüsseln geheimer Informationen

Quantenangriffe könnten verschlüsselte Daten offenlegen, die durch anfällige Public-Key-Schemata in Privatsphäre-Protokollen wie Zcash oder Monero geschützt sind. Sie könnten auch die P2P-Kommunikation in Finanzprotokollen entschlüsseln, sensible Vermögensdetails preisgeben und gezielten Diebstahl ermöglichen.

Umkehren von Hash-Funktionen

Der Grover-Algorithmus könnte Preimage-Angriffe auf Hashes wie SHA-256 beschleunigen, die für Proof-of-Work und die Adressgenerierung verwendet werden.

Dies ist jedoch die am wenigsten besorgniserregende Bedrohung. Viele Post-Quanten-Kryptografie-Schemata enthalten hashbasierte Konstruktionen, da Hashes mit einem ausreichend großen Digest als sicher genug gelten.

Skalierungsherausforderungen in der Post-Quanten-Kryptografie

Während die Post-Quanten-Kryptografie (PQC) wesentlichen Schutz gegen Quantenbedrohungen bietet, führt sie aufgrund des inhärenten Designs dieser Algorithmen zu erheblichen Skalierungshürden. Im Gegensatz zu elliptischen Kurvenschemata, die auf kompakten mathematischen Strukturen beruhen, erfordern PQC-Primitive größere Parameter, um die Sicherheit gegen sowohl klassische als auch Quanten-Angreifer aufrechtzuerhalten. Dies führt zu wesentlich größeren öffentlichen Schlüsseln, privaten Schlüsseln und signature, oft um Größenordnungen.

Die folgende Tabelle illustriert typische Größen für ML-DSA auf einem 128-Bit-Post-Quanten-Sicherheitsniveau im Vergleich zu klassischen Gegenstücken wie 256-Bit-ECDSA:

Algorithmus	Größe öffentlicher Schlüssel (Bytes)	Größe privater Schlüssel (Bytes)	Größe der signature (Bytes)
ML-DSA-87 (Dilithium)	2.592	4.896	4.627
ECDSA (256-Bit)	32	32	65

Wie gezeigt, können ML-DSA-signature über 70-mal größer sein als ECDSA-Äquivalente und öffentliche Schlüssel mehr als 80-mal größer.

Andere PQC-Familien verschärfen dies: Hash-basierte Schemata wie SPHINCS+ können signature von bis zu 41 KB erzeugen, während selbst größenoptimierte Gitter-Varianten wie FALCON immer noch die klassischen Größen um ein Vielfaches überschreiten.

Im Blockchain-Kontext führen diese aufgeblähten Größen zu systemischen Skalierungsproblemen. Größere signature blähen einzelne Transaktionen auf und reduzieren die Transaktionen pro Sekunde (TPS), da Blöcke schneller voll werden und mehr Zeit für die Validierung benötigen. Dies belastet auch die Peer-to-Peer (P2P)-Kommunikation, erhöht den Bandbreitenbedarf und die Ausbreitungsverzögerungen, was das Risiko von Netzwerk-Forks oder verwaisten Blöcken (Orphaned Blocks) in Konsensmechanismen wie Proof-of-Work erhöhen kann. Auch die Speicheranforderungen sind betroffen, was zu höheren Betriebskosten für Nodes und

Barrieren für die Teilnahme führt, insbesondere für Nutzer oder Validatoren mit begrenzten Ressourcen.

Diese Skalierungsherausforderungen müssen in Zukunft von allen Blockchains angegangen werden. Bitcoin zum Beispiel wird weit weniger als 1 TPS haben, wenn die maximale Blockgröße nicht erhöht wird.

Quantus Network Architektur

Post-Quanten-kryptografische Primitive

Quantus Network verwendet **NIST-standardisierte PQC**-Primitive, um die Sicherheit von Transaktionen und Netzwerkkommunikation gegen Quantenbedrohungen zu gewährleisten. Das Herzstück der Transaktionsintegrität ist **ML-DSA (Module-Lattice-based Digital Signature Algorithm**, früher bekannt als CRYSTALS-Dilithium), ein gitterbasiertes Signaturschema, das aufgrund seines Gleichgewichts zwischen Sicherheit, Effizienz und Implementierungsfreundlichkeit ausgewählt wurde. **ML-DSA nutzt die Schwierigkeit von Problemen** wie Learning With Errors (LWE) und Short Integer Solution (SIS) über Modulgitter und bietet robusten Widerstand gegen sowohl klassische als auch Quantenangriffe, einschließlich solcher durch den Shor-Algorithmus.

Für Transaktionssignaturen **integriert Quantus ML-DSA-87**, den Parametersatz, der das höchste Sicherheitsniveau bietet (NIST Security Level 5, entspricht 256-Bit klassischer und 128-Bit Quantensicherheit), um **gegen potenzielle kryptanalytische Durchbrüche bei Gitterproblemen zu schützen**. Diese Wahl priorisiert Vorsicht, da die Gitterkryptografie relativ neu und weniger praxiserprobt ist als klassische Schemata. Die größeren Parameter mildern Risiken durch potenzielle Fortschritte in der Gitterkryptanalyse ab, die kleinere Schlüsselgrößen immer noch als leichtere Ziele belassen würden.

Alternativen

ML-DSA wurde gegenüber Alternativen wie FN-DSA (Falcon) ausgewählt aufgrund von:

- FN-DSAs größerer Implementierungskomplexität (z. B. Erfordernis von Gleitkommaoperationen, die blockchain-unfreundlich sind)
- Fehlen einer deterministischen Schlüsselgenerierung in seiner Spezifikation
- Seinem nicht finalisierten Status zum Zeitpunkt der Entwicklung

Hash-basierte Optionen wie SLH-DSA wurden wegen ihrer noch größeren Signaturgrößen (über 17 KB) verworfen. Crypto-Agility (die Fähigkeit, verschiedene Signaturschemata auszutauschen) ist in Substrate integriert, sodass es relativ einfach ist, diese Alternativen zu einem späteren Zeitpunkt hinzuzufügen, sollten die Umstände dies erfordern.

Während ML-DSA-87 zu größeren Schlüsseln und signature führt, sind diese im frühen Netzwerkstadium von Quantus handhabbar, wo Speicher noch kein Engpass ist und zukünftige Optimierungen wie Wormhole-Adressen über Zero-Knowledge-Beweise die Skalierung adressieren werden.

Technische Details zur Implementierung finden Sie in QIP-0006.

LibP2P

Quantus Network sichert die Peer-to-Peer (P2P) Node-Kommunikation durch eine Kombination aus ML-DSA für die Authentifizierung und ML-KEM (Module-Lattice-based Key Encapsulation Mechanism, früher CRYSTALS-Kyber) für die Verschlüsselung.

Diese Integration erweitert PQC auf den libp2p-Netzwerkstack und modifiziert Kernkomponenten für Quantenresistenz: Verwendung von ML-DSA-87-signature für die Peer-Identität und ML-KEM-768 für die Transportsicherheit (Erweiterung des Noise-Handshakes um eine zusätzliche KEM-Nachricht für quantenresistente Shared Secrets).

Die P2P-Schicht wird in der Quantensicherheitsanalyse oft vernachlässigt. Die Authentifizierung von Peers ist wichtig, aber das Schlimmste, was ein Angreifer auf Peer-Ebene tun könnte, ist, sich als Node auszugeben und ungültige Nachrichten zu senden, was zu einem Denial-of-Service führen könnte. Dieser Angriff wird bereits dadurch gemildert, dass Nodes im Blockchain-Modell generell nicht vertrauenswürdig sind und Nodes ihre Schlüssel leicht wechseln können, wenn der Angriff erkannt wird. Ebenso bringt das Entschlüsseln der P2P-Kommunikation dem Angreifer nur begrenzten Nutzen (z. B. Verfolgung von Transaktionspfaden, gemildert durch Proxys oder Tor), und die meisten Daten werden ohnehin on-chain öffentlich.

Dennoch schützt die quantensichere Sicherung der P2P-Schicht vor Abhören, Man-in-the-Middle-Angriffen und Quantenentschlüsselung und stellt sicher, dass Node-Gossip, Block-Propagation und andere Netzwerkinteraktionen auf absehbare Zeit vertraulich und manipulationssicher bleiben.

Technische Details zur Implementierung finden Sie in QIP-0004.

Skalierung von PQC

Um die der Post-Quanten-Kryptografie inhärenten Skalierungsherausforderungen anzugehen, **führt Quantus Network ein innovatives aggregiertes Post-Quanten-Signaturschema namens „Wormhole Addresses" ein.** Dieses System nutzt Zero-Knowledge-Beweise (ZKPs), die über das Plonky2-Beweissystem (im Grunde STARKs) generiert werden, um die Kontostand-Verifizierung off-chain zu verlagern. Dies

ermöglicht es der chain, einen einzigen kompakten Beweis zu verifizieren, ohne einzelne signature verarbeiten zu müssen.

Wormhole-Adressen ermöglichen die Verifizierung einer großen Anzahl von Transaktionen mit einem einzigen Beweis, wobei die öffentlichen Inputs (z. B. Nullifier, Storage Root, Exit-Adressen und Beträge) zum primären limitierenden Faktor werden. Dies reduziert den amortisierten Speicherbedarf pro Transaktion auf **etwa 256 zusätzliche Bytes pro Transaktion, was viel kleiner ist als jedes bekannte PQC-Signaturschema**.

Die Quantensicherheit des Schemas leitet sich aus der Verwendung der sicheren Hash-Funktion Poseidon2 für Commitments über FRI (Fast Reed-Solomon Interactive Oracle Proofs) ab, anstelle der quantenanfälligen elliptischen Kurven-Pairings, die üblicherweise in SNARKs verwendet werden.

Zusätzlich werden die Authentifizierungsgeheimnisse hinter Poseidon2 verborgen. Da sichere Hash-Funktionen durch den Grover-Algorithmus nur quadratisch geschwächt, aber nicht gebrochen werden, können Hash-Preimage-Beweise als leichtgewichtige Post-Quanten-signature in ZK-Kontexten dienen, ähnlich wie hashbasierte Schemata wie SPHINCS+.

Client / Prover Flow

Nutzer generieren eine nachweislich nicht ausgebbare Adresse durch doppeltes Hashing eines Salts, das mit einem Geheimnis verkettet ist:

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

Diese Konstruktion verhindert falsch-positive Ergebnisse (z. B. die Verwechslung eines einfach gehashten öffentlichen Schlüssels mit einer nicht ausgebbaren Adresse), da in Substrate (und generell) Blockchain-Adressen der einfache Hash eines öffentlichen Schlüssels sind, der aus dem privaten Schlüssel über eine algebraische Operation abgeleitet wird, nicht über einen sicheren Hash. Die Sicherheit der Konstruktion reduziert sich daher auf das Finden des Preimage-eines-Preimages eines sicheren Hashes. Token, die an diese Adresse gesendet werden, werden effektiv verbrannt. Sie können nicht ausgegeben werden, da kein privater Schlüssel für die Adresse existiert, die sie empfangen hat. Diese Coins können daher neu geprägt (re-minted) werden, ohne das Angebot aufzublähen.

Für jede Überweisung wird ein TransferProof-Speicherobjekt erstellt, das Details wie einen eindeutigen globalen Überweisungszähler enthält. Das Wallet des Nutzers

generiert einen Merkle-Patricia-Trie (MPT) Speicherbeweis vom Storage Root eines aktuellen Block-Headers zum Leaf für diesen TransferProof.

Ein Nullifier wird berechnet:

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

Um Double-Spends zu verhindern, wobei das Geheimnis deterministisch aus dem Wallet-Seed zur Aufbewahrung abgeleitet wird.

Aggregator Flow

Jede Partei (Client, Miner oder Drittanbieter) kann mehrere Beweise unter Verwendung der Rekursion von Plonky2 aggregieren und so einen Baum von Beweisen bilden, bei dem jeder Elternbeweis eine Verifizierung der Kinderbeweise ist, wobei die öffentlichen Inputs der Kinderbeweise aggregiert werden:

- Nullifier werden unverändert weitergegeben
- Exit-Adressen werden dedupliziert
- Block-Hashes werden als verknüpft nachgewiesen und dann werden alle außer dem aktuellsten verworfen
- Beträge für doppelte Exit-Adressen werden summiert Diese Rekursion unterstützt die hierarchische Aggregation und reduziert die On-Chain-Daten drastisch.

Chain / Verifier Flow

Das Netzwerk verifiziert den aggregierten Beweis durch Prüfung von:

- Block-Hash ist on-chain und aktuell
- Eindeutigkeit des Nullifiers (um Double-Spends zu verhindern)
- Gültigkeit des Beweises

Die ZK-Schaltung erzwingt:

- Korrektheit des Speicherbeweises
- Genauigkeit der Nullifier-Berechnung
- Nicht-Ausgebbarkeit der Adresse
- Übereinstimmung des Kontostands zwischen Inputs und Outputs
- Verknüpfung der Block-Header

Plonky2 wurde aus folgenden Gründen ausgewählt:

- bereits auditiert
- post-quantensicher
- kein Trusted Setup erforderlich
- effiziente Beweiserstellung/Verifizierung
- nahtlose Beweisaggregation
- Rust-native Implementierung
- kompatibel mit der no-std-Umgebung von Substrate

Zu den Performance-Highlights gehören:

Rekursive Beweise in 170 Millisekunden und kompakte Größen (100 KB pro aggregiertem Beweis), was massive Durchsatzsteigerungen ermöglicht.

In einem optimalen Fall mit 5-MB-Blöcken und allen Transaktionen an denselben Output könnten **Wormhole-Adressen ca. 153.000 Transaktionen in einen einzigen Block packen** (4,9 MB / 32 Bytes pro Nullifier), eine 223-fache Verbesserung gegenüber ca. 685 rohen ML-DSA-Transaktionen (5 MB / jeweils 7,3 KB).

Sicherheitshinweise

Potenzielle Risiken umfassen Inflationsbugs durch fehlerhafte Schaltungs-/Verifizierungsimplementierungen, obwohl dies wirtschaftlich erkennbar wäre, wenn neu geprägte Coins die Guthaben von Null-Sende-Adressen übersteigen. Nutzer können optional beweisen, dass eine Adresse ein Wormhole ist, indem sie den ersten Hash veröffentlichen, ohne das Geheimnis preiszugeben. Verifizierungstransaktionen sind unsigniert, daher muss Denial-of-Service durch fehlgeschlagene Transaktionen nicht-finanziell gemildert werden. Die Berechnungen des Token-Angebots bleiben erhalten, da Neugeprägte als neue Coins erscheinen, aber die Garantien für das maximale Angebot über Burns aufrechterhalten werden.

Weitere technische Details zur Implementierung finden Sie in QIP-0005.

Konsensmechanismus

Quantus Network verwendet einen Proof-of-Work (PoW) Konsensalgorithmus, der die wünschenswerten Eigenschaften des Bitcoin-Konsensalgorithmus beibehält und gleichzeitig die Kompatibilität mit ZK-Beweissystemen verbessert, indem SHA-256 durch Poseidon2 ersetzt wird.

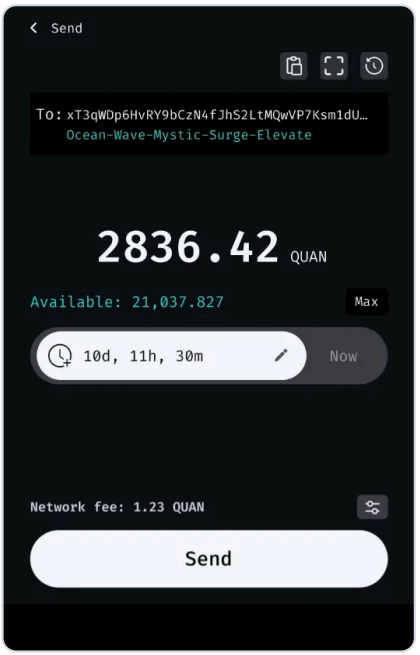
Wichtig ist, dass diese Änderung nicht aus Gründen der Quantensicherheit erfolgt. Kryptografische Hash-Funktionen wie SHA-256 werden durch Quantenalgorithmen, insbesondere Grover, geschwächt, aber nicht zerstört. Einige Post-Quanten-Signaturschemata verwenden aus diesem Grund sichere Hashes als Baustein.

Poseidon2 ist eine Weiterentwicklung der Poseidon-Hash-Funktion. Das Erstellen von SNARKs oder STARKs für Berechnungen mit traditionellen Hash-Funktionen wie SHA-256 erfordert oft fast 100-mal so viele Gatter im Vergleich zur Verwendung von Poseidon, das vollständig auf algebraischen Funktionen über Feldelementen beruht, anstatt auf Operationen auf Bitebene. Wir verwenden das Goldilocks-Feld sowohl für Poseidon2 als auch für Plonky2, um die Effizienz zu maximieren.

Vermögenserhaltung

Bei der Verwaltung von Kryptowährungsschlüsseln gibt es viele Risiken. Die meisten davon sind vermeidbar. Quantus Network integriert Benutzerfreundlichkeit direkt in die chain selbst und ermöglicht es auch Laien, beruhigt Transaktionen durchzuführen.

Reversible Transaktionen

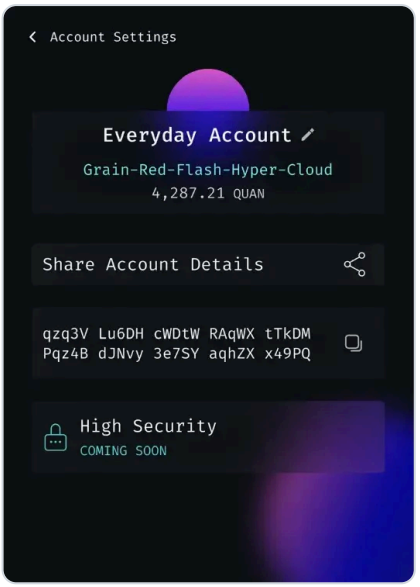


Quantus Network bietet benutzerkonfigurierbare reversible Transaktionen an, die es Sendern ermöglichen, ein Zeitfenster festzulegen, in dem sie ausgehende Überweisungen stornieren können. Dies verbessert die Diebstahlsabschreckung und Fehlerkorrektur, ohne die grundlegende Irreversibilität der Blockchain zu opfern. Unter Nutzung eines modifizierten Substrate „Scheduler Pallets", das Zeitstempel für intuitive Verzögerungen verwendet, ermöglicht das System den Clients, Überweisungen über eine einfache Schnittstelle zu planen. In den Wallets werden Countdowns sowohl für den Sender (mit einem Abbrechen-Button) als auch für den Empfänger (Anzeige des Abschlusses, wenn nicht storniert) angezeigt. Dies balanciert schnelle Finalität für den Handel mit Flexibilität für Nutzer aus, die besorgt sind, Fehler zu machen oder eine Anzahlung in gutem Glauben ohne Treuhandservice leisten möchten.

Reversible Transaktionen bilden einen leistungsstarken Baustein für neuartige Sicherheitsprotokolle, während die Dezentralisierung durch On-Chain-Durchsetzung gewahrt bleibt.

Weitere technische Details finden Sie in QIP-0009.

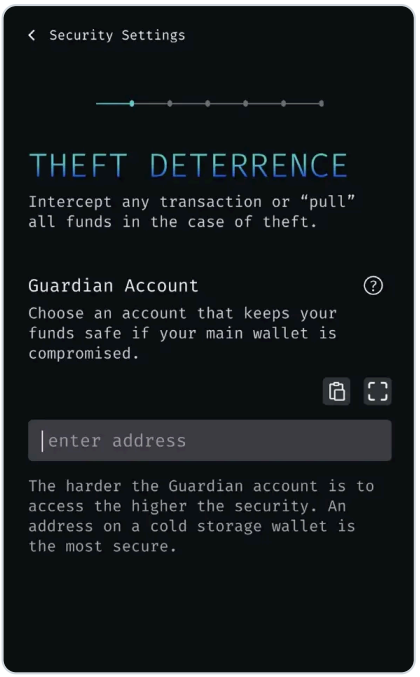
Check-Phrases



Quantus Network führt „check-phrases" ein, eine kryptografisch sichere, für Menschen lesbare Prüfsumme für Blockchain-Adressen und andere Daten, die eine menschliche Verifizierung erfordern. **Durch das Hashen der Adresse zur Erzeugung einer kurzen Sequenz einprägsamer Wörter aus der BIP-39-Mnemonic-Liste ermöglichen check-phrases schnelle, fehlerfreie Integritätsprüfungen und schützen vor Tippfehlern, Manipulationen und Angriffen wie Address Poisoning**. Dieses Tool ermöglicht es Nutzern, Adressen während Überweisungen sicher zu verifizieren, ohne sich auf verkürzte Anzeigen oder schwache Prüfsummen verlassen zu müssen. Eine Schlüsselableitungsfunktion mit 50.000 Iterationen wird verwendet, um sicherzustellen, dass das Erstellen einer Rainbow Table für gegebene Prüfsummen sehr teuer ist. Natürlich sollten Nutzer bei großen Transaktionen weiterhin jeden Buchstaben der Adresse manuell auf Richtigkeit prüfen.

Weitere technische Details finden Sie in QIP-0008.

Hochsicherheitskonten



Quantus Network bietet die Möglichkeit, jedes Konto zu einem „Hochsicherheitskonto" aufzuwerten, das obligatorische Stornierungsfristen für alle ausgehenden Überweisungen erzwingt. Dies ermöglicht es einem benannten „Guardian"-Konto, wie z. B. einem Hardware-Wallet, einem Multisig oder sogar einem vom Nutzer gewählten vertrauenswürdigen Dritten, verdächtige Transaktionen während der Stornierungsfrist exklusiv zu stornieren. Dabei werden die Gelder an den Guardian gesendet statt an den Sender oder Empfänger. Diese optionale, permanente Funktion baut auf reversiblen Überweisungen auf, bei denen Nutzer bei der Aktivierung die Verzögerung und den Interzeptor festlegen, was Diebe daran hindert, die Funktion zu deaktivieren.

Der Interzeptor kann selbst ein weiteres Hochsicherheitskonto mit eigenem Guardian sein, was komponierbare Hierarchien ermöglicht, in denen jeder Guardian übergeordnete Berechtigungen für das von ihm geschützte Konto hat. Dieses Design ahmt gerichtlich angeordnete Rückbuchungen im traditionellen Finanzwesen nach, jedoch unter der Kontrolle des Nutzers. Es balanciert Sicherheit und Komfort für hochwertige Konten aus und gibt Zeit, unbefugte Aktivitäten zu erkennen und darauf zu reagieren, ohne die Blockchain-Finalität für legitime Abläufe zu beeinträchtigen.

Weitere technische Details finden Sie in QIP-0011.

Schlüsselwiederherstellung

Viele Krypto-Vermögen sind mit ihren Besitzern ins Grab gegangen. Quantus Network bietet eine einfache Möglichkeit, eine Wiederherstellungsadresse anzugeben, die Ihr Guthaben jederzeit abheben kann, vorbehaltlich einer festen Verzögerung. Während dieser Zeit kann der Besitzer die Wiederherstellung ablehnen, wenn er Zugriff auf den Schlüssel hat. Diese Funktion ermöglicht die Nachfolge: Nutzer haben ein On-Chain-Testament ohne die Notwendigkeit von Gerichten oder Nachlässen.

HD-Lattice

Hierarchical Deterministic (HD) Wallets sind der Industriestandard für Blockchains. Sie ermöglichen es Nutzern, eine einzige Seed-Phrase für alle Schlüssel zu sichern, was die Sicherheit und den Komfort gegenüber manuellen Backups pro Aktion verbessert.

Die Anpassung an Gitter-Schemata wie Dilithium bringt zwei Herausforderungen mit sich:

- HMAC-SHA512-Outputs können nicht direkt Gitter-Privatschlüssel bilden, da diese „gute Basis"-Polynome über Rejection Sampling erfordern.
- Die nicht-gehärtete (non-hardened) Schlüsselableitung beruht auf elliptischer Kurvenaddition, die in Gittern fehlt (öffentliche Schlüssel sind unter keiner algebraischen Operation abgeschlossen).

Quantus Network adressiert das erste Problem, indem es den Output des HMAC als Entropie verwendet, um den privaten Schlüssel deterministisch zu konstruieren, statt als den privaten Schlüssel selbst. Das zweite Problem ist weniger kritisch und es bleibt eine offene Forschungsfrage, ob die Gitterkryptografie angepasst werden kann, um es zu adressieren.

Weitere technische Details finden Sie in QIP-0002.

Tokenomics und Governance

Quantus Network existiert in einem sich verändernden Umfeld, und wir können nicht davon ausgehen, dass wir beim ersten Versuch alles richtig machen werden. Aus diesem Grund wählen wir einen einfachen Ausgangspunkt und erlauben dem Governance-System, Änderungen vorzunehmen, sobald neue Informationen vorliegen. Dieses Design macht die Blockchain zu einer lebendigen Einheit, die sich nach Belieben an ihre Umgebung anpassen kann. Insbesondere der Substrate-Governance-Prozess ermöglicht tiefgreifende Änderungen an der chain mit minimaler Koordination unter den verschiedenen Node-Betreibern.

Block-Belohnungen

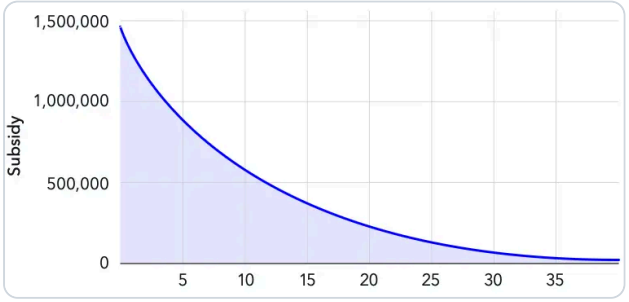
Quantus Network verwendet ein einfaches Tokenomics-Modell, das dem von Bitcoin nachempfunden ist. Es gibt ein maximales Angebot von 21.000.000 Coins und eine einfache Heuristik bestimmt die Belohnung pro Block.

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

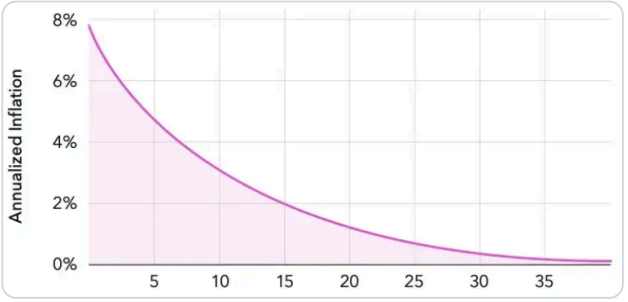
Diese Heuristik bildet eine glatte, exponentiell abfallende Kurve, da der block_reward zum current_supply beiträgt, was den beim nächsten Block berechneten block_reward reduziert.

Jegliche Burns aus Gebühren oder anderweitig reduzieren den current_supply und werden im Wesentlichen Teil des Budgets für Block-Belohnungen. Die Konstante ist so gewählt, dass bei Abwesenheit von Burns 99 % der Coins in etwa 40 Jahren emittiert werden.

Block-Belohnungen / Jahr



Inflation / Jahr



Investoren-Allokation

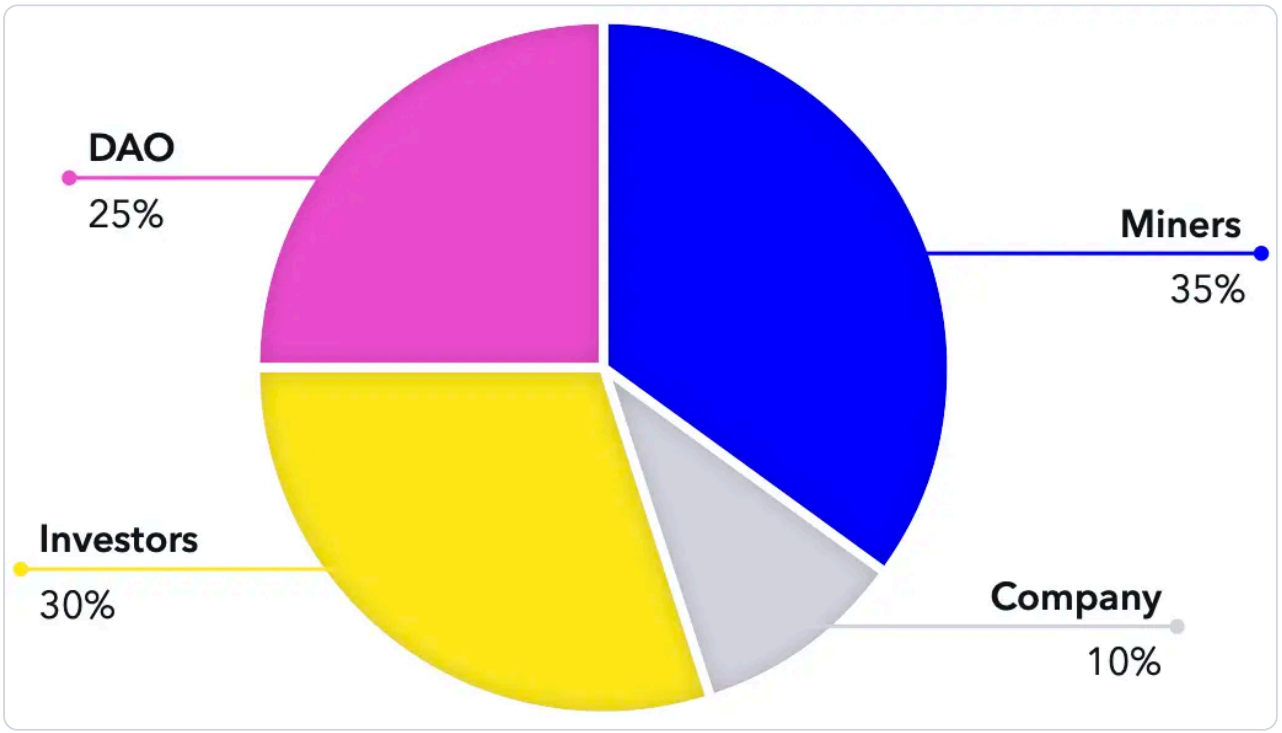
Quantus Network wurde mit Hilfe von Angel-Investoren aufgebaut, die ein großes Risiko bei der Finanzierung eingegangen sind. Um die Angebotsüberhänge zu vermeiden, die Investoren-Lockups erzeugen, machen wir alle Investoren, ob öffentlich oder privat, vom ersten Tag an liquide. Diese Allokation wird das einzige „Pre-Mine" sein. Alle anderen Token müssen durch Mining erschaffen werden. Je nach Erfolg der öffentlichen Verkäufe wird dieser Anteil 20–30 % des Gesamtangebots ausmachen.

Unternehmens-Allokation

Um das Team für das Risiko zu entschädigen, neue Technologie ohne Erfolgsversprechen zu bauen, werden wir die Block-Belohnungen in zwei Hälften teilen. Die erste Hälfte geht an den Miner. Für etwa vier Jahre geht die zweite Hälfte an das Unternehmen. Dies ergibt einen De-facto-Vesting-Plan von etwa 10 % des Gesamtangebots für das Unternehmen. Während dieser Zeit erhalten die Miner die gleiche Menge an neu geprägten Coins.

Nach diesem Zeitpunkt wird der Anteil des Unternehmens an den Block-Belohnungen an eine von Token-Inhabern verwaltete Treasury umgeleitet, was im Wesentlichen eine DAO bildet.

Ungefähre Angebotsallokation



Transaktionsgebühren

Standardtransaktionen haben eine Gebühr, die an die Miner geht und einen Anreiz bietet, Transaktionen aufzunehmen. Stornierte Transaktionen von Hochsicherheitskonten werden mit einer volumenbasierten Gebühr von 1 % belastet, die aufgeteilt wird: Die Hälfte geht an den Miner und die Hälfte wird verbrannt (Burn) und fließt in das zukünftige Sicherheitsbudget. Transaktionen, die über das ZK-Aggregationssystem laufen, unterliegen ebenfalls einer volumenbasierten Gebühr von 0,1 %, die zwischen dem Miner, dem Beweis-Aggregator und einem Burn aufgeteilt wird.

Forkless Upgrades

Quantus Network unterstützt „forkless" Upgrades durch Substrate-Runtime-Upgrades. Dies ermöglicht es der Kernlogik der Blockchain (der „Runtime"), sich weiterzuentwickeln, ohne dass Hard Forks erforderlich sind, die das Netzwerk stören oder die Community spalten könnten. Dies wird über On-Chain-Governance-Referenden erreicht, bei denen genehmigte Vorschläge einen Runtime-Swap auslösen. Dabei wird im Wesentlichen der bestehende WASM-Code-Blob in einem einzigen Block durch einen neuen ersetzt, was die Kontinuität von Zustand und Betrieb gewährleistet. Dieser Upgrade-Pfad minimiert Ausfallzeiten und Risiken und ermöglicht es der Community, das Protokoll iterativ zu verfeinern.

Governance-System

Quantus Network übernimmt sein Governance-Framework vom OpenGov-System von Polkadot über Substrate. Token-Inhaber nehmen über Conviction Voting teil, wobei sie zustimmen, ihre Assets für unterschiedliche Zeiträume zu sperren, um das Gewicht ihrer Stimme zu verstärken. Diese Verstärkung kann von 1x (keine Sperre) bis 6x (maximale Sperre) reichen. Dieses Design fördert die langfristige Ausrichtung, indem Einfluss an Engagement gebunden wird.

Vorschläge werden in mehrere Abstimmungstracks unterteilt, die „Origins" genannt werden. Jede Origin hat maßgeschneiderte Parameter wie Zustimmungsschwellen (z. B. Supermajorität für weitreichende Änderungen), Mindesteinlagen zur Abschreckung von Spam, Vorbereitungs-/Inkrafttretensfristen und Entscheidungszeitpläne zur Vermeidung von Stillstand. Dieses Multi-Track-Design ermöglicht die parallele Bearbeitung verschiedener Referenden, von routinemäßigen Treasury-Ausgaben bis hin zu kritischen Runtime-Upgrades.

Das Technical Collective ist eine ausgewählte Gruppe von technischen Experten, die als Fachgremium fungieren, um dringende technische Angelegenheiten vorzuschlagen, zu

prüfen oder auf eine Whitelist zu setzen. Diese werden über einen speziellen Track beschleunigt bearbeitet, während die Aufsicht durch die Community gewahrt bleibt.

Quantus übernimmt dieses System ohne Modifikationen, startet jedoch mit einem minimalistischen Setup, um Komplexität in der Anfangsphase zu vermeiden. Zunächst ist nur der Technical Collective Track aktiv, der für verbindliche, hochprivilegierte Entscheidungen wie Protokoll-Upgrades oder Parameteranpassungen genutzt wird.

Später werden wir einen unverbindlichen Community-Abstimmungstrack einführen, um die Stimmung zu nicht durchsetzbaren Themen wie Feature-Vorschlägen oder Ökosystem-Umfragen zu messen. Dieses System wird verbindlich, wenn das Unternehmen das Netzwerk an die DAO übergibt.

Dieser phasenweise Ansatz ermöglicht es dem Netzwerk, sich organisch über zukünftige Governance-Abstimmungen zu entwickeln, ohne die Nutzer zu Beginn mit unnötiger Komplexität zu belasten.

Roadmap

Heisenberg Inception

DEZEMBER 2024

Finanzierung gesichert, Substrate gewählt

Resonance Alpha

JULI 2025

Öffentliches Testnet, Dilithium-Signaturen, Reversible Transaktionen

Schrödinger Beta

OKTOBER 2025

Features vollständig, bereit für Audit

Dirac Beta

NOVEMBER 2025

PoW auf Poseidon2 umgestellt, Audits adressiert

Planck Beta

JANUAR 2026

Hochsicherheitskonten, Multisigs, Hardware-Wallet

Bell Mainnet

Q1 2026

Mainnet-Start

Fermi Upgrade

Q2 2026

ZK-Aggregation

Risiken

Der Aufbau von Quantus Network ist mit inhärenten Risiken verbunden.

- **Implementierungsprobleme:** Fehler in der Softwarelogik können selbst in den am besten konzipierten Systemen zu schwerwiegenden Ausfällen führen.
- **Probleme bei der NIST-Algorithmenauswahl:** Potenzielle Schwachstellen oder Backdoors in den ausgewählten Post-Quanten-Standards (z. B. ML-DSA, ML-KEM), die nach der Standardisierung auftreten könnten. Im schlimmsten Fall würden solche Schwachstellen es einem Angreifer ermöglichen, signature zu fälschen, indem er einen privaten Schlüssel aus dem öffentlichen ableitet, was einen katastrophalen Ausfallmodus der chain darstellt. Sollten solche Schwachstellen öffentlich werden, könnte Quantus Network auf einen neuen Algorithmus aufgerüstet werden. Wenn solche Schwachstellen jedoch nur spärlich ausgenutzt werden, werden sie möglicherweise nie entdeckt.
- **Quantencomputing-Zeitpläne:** Quantendurchbrüche könnten viel später als erwartet eintreten, was die Notwendigkeit für PQC verzögert. Umgekehrt könnte eine geheimnisvolle Entwicklung (z. B. durch Regierungen) zu plötzlichen Bedrohungen führen, wenn die Blockchain-Community es versäumt, schnell Upgrades durchzuführen.
- **Andere Überlegungen:** Allgemeine Adoptionsbarrieren, regulatorische Unsicherheiten im Finanz-/Blockchain-Bereich und die inhärente Volatilität von Krypto-Ökosystemen.

Schlusswort

QUANTUS

Wir glauben an die Kraft offener Protokolle, Proof-of-Work und souveränes Eigentum. Die Quantus Network App, verfügbar für Desktop und Mobilgeräte, ermöglicht es Nutzern, digitale Assets zu speichern, neue Blöcke zu minen und an einer faireren finanziellen Zukunft ohne Zwischenhändler teilzunehmen.

Wir setzen uns für Transparenz, Privatsphäre und die Stärkung des Einzelnen durch sichere Self-Custodial-Tools ein.