quantus

quantensicher, verschlüsseltes geld

VERÖFFENTLICHT
21. märz 2026

VERSION
0.3.3

KLASSIFIZIERUNG
public

Dieses Whitepaper dient ausschließlich Informationszwecken und stellt weder ein Angebot zum Verkauf noch eine Aufforderung zum Kauf noch eine Empfehlung für Wertpapiere, Anlagen oder Finanzprodukte dar. Leserinnen und Leser sollten eigene Sorgfalt walten lassen und qualifizierte Fachleute konsultieren, bevor sie Anlageentscheidungen treffen. Quantus Network übernimmt keine Zusicherungen oder Gewährleistungen hinsichtlich der Richtigkeit oder Vollständigkeit der hier enthaltenen Informationen.

INHALT

01

einführung

die quantenbedrohung

Klassische Blockchains stehen vor einer existenziellen Bedrohung durch kryptographisch relevante Quantencomputer (CRQC). Die kryptographischen Grundlagen von Blockchains beruhen auf der Schwierigkeit des diskreten Logarithmusproblems (DLP), und Quantenalgorithmen, insbesondere der von Shor, können das DLP exponentiell schneller lösen als klassische Computer. Diese Schwachstelle könnte es quantenbezogenen Angreifern ermöglichen, private aus öffentlichen Schlüsseln abzuleiten – womit sie Transaktionen fälschen und sensible Finanzdaten entschlüsseln könnten.

> ohne proaktive quantenresistente Upgrades riskiert die Billionen-Dollar-Kryptoökonomie eine plötzliche Abwertung durch solche Angriffe.

einzigartiges wertversprechen

Nach dem lateinischen Wort für „wie viel“ benannt, ermöglicht Quantus Network skalierbares, quantensicheres, privates Geld. Quantus ist keine allgemeine Smart-Contract-Plattform. Wie ein Restaurant mit wenigen hoch verfeinerten Gerichten bietet Quantus:

— Post-Quanten-Signaturen für alle Transaktionen

— Post-Quanten-Signaturen und -Verschlüsselung (ML-DSA und ML-KEM) zur Absicherung von Peer-to-Peer-Verbindungen

— Post-Quanten-Zero-Knowledge-Beweise zur Skalierung

— Hochsicherheitskonten, um Diebstahl zu erschweren und Fehlerkorrektur zu ermöglichen

— Lesbare Prüfsätze zur einfachen Adressverifikation

Die Konzentration auf skalierbares, quantensicheres, privates Geld ergibt sich aus der Bedrohung durch CRQC für die Branche und aus der Unfähigkeit von Bitcoin, diese Herausforderungen zu adressieren.

02

die quantenbedrohung für die blockchain

grundlagen des quantencomputings

Quantencomputer nutzen Prinzipien wie Superposition und Verschränkung, um Berechnungen durchzuführen, die für klassische Maschinen unhandelbar sind. Anders als klassische Bits, die 0 oder 1 sind, können Qubits gleichzeitig in mehreren Zuständen existieren, was für bestimmte Probleme exponentiellen Parallelismus ermöglicht. Diese Fähigkeit birgt existenzielle Risiken für die kryptographischen Systeme, die Blockchain-Finanzen tragen, da für Quantenhardware entwickelte Algorithmen die Sicherheitsannahmen der meisten Public-Key-Kryptographie untergraben.

Shors Algorithmus, 1994 von Peter Shor vorgestellt, liefert ein polynomzeitverfahren zur Faktorisierung großer Ganzzahlen und zur Lösung des diskreten Logarithmusproblems auf einem Quantencomputer. Er nutzt Quanten-Fourier-Transformationen (QFT), um die Periode einer Funktion zu finden, und kann damit effizient die Einwegfunktionen invertieren, auf denen Verfahren wie RSA oder Elliptische-Kurven-Kryptographie (ECC) beruhen. Für Blockchain-Finanzen bedeutet das: Ein Angreifer mit einem ausreichend leistungsfähigen Quantencomputer (geschätzt ~2.000

logische Qubits [6][7][8][9]) könnte private aus öffentlichen Schlüsseln in polynomieller Zeit $O(n^3)$ ableiten – eine extreme Beschleunigung, die verwundbare Systeme über Nacht obsolet macht. [1]

Grovers Algorithmus, 1996 von Lov Grover vorgeschlagen, liefert eine quadratische Beschleunigung für unstrukturierte Suche und reduziert die Suchzeit von $O(n)$ auf $O(\sqrt{n})$ Operationen. Obwohl er für asymmetrische Kryptographie nicht so verheerend ist wie Shor, betrifft Grover symmetrische Primitive wie Hashfunktionen und AES-Verschlüsselung, wodurch das Sicherheitsniveau effektiv halbiert wird (z. B. verhält sich ein 256-Bit-Schlüssel gegenüber Quantenangriffen wie 128 Bit). Dieser Angriff wird durch Verdopplung der Bit-Sicherheit statt durch einen Wechsel des kryptographischen Schemas gemildert. Zudem ist Grovers quadratische Beschleunigung wegen hoher Qubit- und Gatteranforderungen praktisch wenig relevant: Sie erfordert Milliarden sequenzieller Operationen bei begrenzter Parallelisierung, was sie selbst mit zukünftiger Hardware für reale Investitionen unattraktiv macht. [2]

vier bedrohungskategorien

01 - digitale signaturen fälschen

Shors Algorithmus bedroht direkt die auf ECC basierenden Signaturen, die in den meisten Blockchains verwendet werden (z. B. die Kurve secp256k1 bei Bitcoin), und erlaubt es Angreifern, Nutzer

zu imitieren und betrügerische Transaktionen zu autorisieren. Eine solche Fähigkeit wäre ein kritisches Versagen der grundlegendsten Eigenschaft einer Blockchain.

02 - falsche beweise in zero-knowledge-systemen fälschen

Viele Zero-Knowledge-Beweise, etwa zk-SNARKs für datenschutzorientierte Finanzen, beruhen auf der Schwierigkeit des diskreten Logarithmus über Elliptische-Kurven-Paarungen für Commitments. Shor könnte es ermöglichen, ungültige Beweise zu erzeugen, die gültig erscheinen – womit ein Angreifer neue Coins prägen oder den Zustand von Layer-2-Lösungen (L2) fälschen könnte.

03 - geheime information entschlüsseln

Quantenangriffe könnten durch verwundbare Public-Key-Schemata geschützte Daten in Datenschutzprotokollen wie Zcash oder Monero offenlegen. Sie könnten auch P2P-Kommunikation in Finanzprotokollen entschlüsseln, sensible Vermögensdetails preisgeben und gezielten Diebstahl ermöglichen.

04 - hashfunktionen invertieren

Grovers Algorithmus könnte Preimage-Angriffe auf Hashes wie SHA-256 beschleunigen, die in Proof-of-Work und Adressgenerierung verwendet werden – das ist jedoch die am wenigsten besorgniserregende Bedrohung. Viele Post-Quanten-Kryptographie-Schemata nutzen hashbasierte Konstruktionen, da

Hashes mit ausreichend großem Digest als hinreichend sicher gelten.

skalierungsherausforderungen in der post-quanten-kryptographie

Obwohl Post-Quanten-Kryptographie (PQC) wesentlichen Schutz vor Quantenbedrohungen bietet, führt sie aufgrund des inhärenten Designs dieser Algorithmen zu erheblichen Skalierungshindernissen. Anders als Elliptische-Kurven-Verfahren, die auf kompakten mathematischen Strukturen beruhen, benötigen PQC-Primitive größere Parameter, um die Sicherheit gegen klassische und quantenbezogene Angreifer zu halten. Dadurch entstehen deutlich größere öffentliche und private Schlüssel sowie Signaturen, oft um Größenordnungen. Die folgende Tabelle zeigt typische ML-DSA-Größen bei einer Post-Quanten-Sicherheit von 128 Bit im Vergleich zu klassischen Äquivalenten wie 256-Bit-ECDSA: [10]

ALGORITHMUS	ÖFFENTLICHER SCHLÜSSEL	PRIVATER SCHLÜSSEL	SIGN
ML-DSA-87 (Dilithium)	2,592 bytes	4,896 bytes	4,627 bytes
ECDSA (256-bit)	32 bytes	32 bytes	65 by

Größen bei Post-Quanten-Sicherheit von 128 Bit. Quelle: Open Quantum Safe Project [10]

Wie zu sehen ist, können ML-DSA-Signaturen mehr als 70-mal größer sein als vergleichbare ECDSA-Signaturen, öffentliche Schlüssel mehr als 80-mal. Andere PQC-Familien verschärfen das: hashbasierte Schemata wie SPHINCS+ können Signaturen bis zu 41 KB erzeugen, während größenoptimierte Gittervarianten wie FALCON die klassischen Größen weiterhin um ein Vielfaches übertreffen.

In Blockchain-Kontexten summieren sich diese aufgeblähten Größen zu systemischen Skalierungsproblemen. Größere Signaturen blähen einzelne Transaktionen auf, senken die Transaktionen pro Sekunde (TPS), weil Blöcke schneller voll werden und die Validierung länger dauert. Sie belasten auch die Peer-to-Peer-Kommunikation (P2P), erhöhen Bandbreite und Propagationsverzögerungen und können das Risiko von Forks oder Waisenblöcken in Konsensmechanismen wie Proof-of-Work erhöhen. Auch die Speicheranforderungen steigen, mit höheren Betriebskosten für Knoten und Hürden für die Teilnahme, insbesondere für Nutzer oder Validatoren mit begrenzten Ressourcen.

> **HINWEIS**
>
> Diese Skalierungsherausforderungen müssen künftig alle Blockchains angehen. Bitcoin hätte

> zum Beispiel deutlich weniger als 1 TPS, wenn die maximale Blockgröße nicht erhöht würde.

03

die migrationskrise

das koordinationsproblem

Die konservative Kultur von Bitcoin lehnt Protokolländerungen ab. Jede PQC-Verbesserung würde Konsens zu kontroversen Fragen wie Migrationsfristen, möglichem Coin-Beschlagnahme und Erhöhungen der Blockgröße erfordern. Selbst wenn die Community zustimmte, müsste jeder Nutzer seine Coins auf neue quantensichere Adressen migrieren. Die Migration erfordert Handeln aller Krypto-Inhaberinnen und -Inhaber, von denen viele den Zugang zu Wallets verloren haben oder die Bedrohung ignorieren.

Diese Probleme bestehen in jeder öffentlichen Blockchain, sind für Bitcoin aber besonders schwer wegen fehlender klarer Führung und einer Philosophie technischer Versteinerung.

das problem verlorener coins

Schätzungen zufolge sind zwischen 250 und 500 Milliarden US-Dollar in Bitcoin dauerhaft unzugänglich wegen verlorener Schlüssel, verstorbener Inhaber oder vergessener Wallets. [3] Diese Coins können nicht migriert werden und wirken wie eine öffentliche Belohnung für den Bau eines kryptographisch relevanten Quantencomputers (CRQC). Quantenangreifer werden

private Schlüssel aus nicht migrierten öffentlichen Schlüsseln ableiten und vermutlich Milliarden an BTC auf den Markt drücken.

> die einzige technische Lösung erfordert eine strikte Frist, die nicht migrierte Coins einfriert – eine politische Unmöglichkeit.

Ohne eine solche Frist werden nicht migrierte Coins gestohlen und verkauft, der Markt gedrückt und das Vertrauen in das Netz zerstört.

das problem des migrationszeitplans

Post-Quanten-Signaturen sind 20- bis 80-mal größer als die aktuellen Bitcoin-Signaturen. Ohne grundlegende Architekturänderungen bricht die Leistung von Bitcoin auf einen Bruchteil seiner ohnehin begrenzten Kapazität ein.

Selbst wenn Bitcoin die politischen und technischen Hürden löst, würde die Migration selbst Monate oder Jahre dauern. Jede Inhaberin und jeder Inhaber muss mindestens eine Transaktion senden, um Mittel auf eine quantensichere Adresse zu verschieben. Viele werden zuerst Testtransaktionen senden. Während aufgeblähte PQC-Signaturen die Leistung erdrücken, entsteht eine Warteschlange über Monate oder Jahre, während weiterhin verwundbare Coins exponiert sind.

> **DIE ANTWORT VON QUANTUS**

> Diese sich stapelnden Herausforderungen machen es außerordentlich schwer, Quantensicherheit zu bestehenden Ketten hinzuzufügen. Quantus Network vermeidet das, indem es Quantensicherheit von Tag eins in die Kette integriert.

04

architektur von quantus network

grundlagen

Quantus Network basiert auf Substrate, einem Blockchain-SDK, entwickelt von Parity Technologies, dem Team hinter Ethereum und Polkadot. Substrate ist hochgradig modular, sodass Komponenten leicht ausgetauscht werden können, um den Fokus auf das zu legen, was Quantus einzigartig macht.

Quantus erweitert Substrate:

— durch Unterstützung für Post-Quanten-Signaturschemata

— durch Aktualisierung der P2P-Netzwerksicherheit auf Post-Quanten

— durch hinzugefügte, nutzergesteuerte Transaktionsumkehrbarkeit

— durch ZK-kompatible Datenbank, indem alle Datentypen an Feldelement-Grenzen ausgerichtet werden

post-quanten-kryptographische primitive

Quantus Network setzt vom NIST standardisierte PQC ein, um Transaktions- und Netzwerkkommunikationssicherheit gegen Quantenbedrohungen zu gewährleisten. Im Kern der

Transaktionsintegrität steht **ML-DSA** (Module-Lattice-Based Digital Signature Algorithm, zuvor CRYSTALS-Dilithium), ein gitterbasiertes Signaturschema, das für sein Gleichgewicht aus Sicherheit, Effizienz und Implementierbarkeit gewählt wurde. ML-DSA nutzt die Schwierigkeit von Problemen wie Learning With Errors (LWE) und Short Integer Solution (SIS) über Modulgittern und bietet robusten Widerstand gegen klassische und quantenbezogene Angriffe, einschließlich Shors Algorithmus. [4]

Für Transaktionssignaturen integriert Quantus **ML-DSA-87**, den Parametersatz mit der höchsten Sicherheitsstufe (NIST Level 5, äquivalent zu 256 Bit klassisch und 128 Bit quantenbezogen), um mögliche Fortschritte in der Gitter-Kryptoanalyse abzufedern. Diese Wahl priorisiert Vorsicht, da Gitter-Kryptographie relativ neu und weniger kampferprobt ist als klassische Schemata. Größere Parameter mildern Risiken potenzieller Fortschritte in der Gitter-Kryptoanalyse, die kleinere Schlüsselgrößen weiterhin als schwächere Ziele lassen würden.

in betracht gezogene alternativen

ML-DSA wurde gegenüber Alternativen wie FN-DSA (Falcon) gewählt wegen der höheren Implementationskomplexität von FN-DSA (z. B. erfordert Gleitkommaoperationen, wenig geeignet für Blockchain), fehlender deterministischer Schlüsselerzeugung in der Spezifikation und des zum Entwicklungszeitpunkt nicht finalisierten Status.

Hashbasierte Optionen wie SLH-DSA wurden wegen noch größerer Signaturen (über 17 KB) nicht gewählt. Krypto-Agilität (die Fähigkeit, Signaturschemata auszutauschen) ist in Substrate integriert, sodass diese Alternativen künftig relativ einfach ergänzt werden können, wenn die Umstände es erfordern.

Obwohl ML-DSA-87 größere Schlüssel und Signaturen erzeugt, sind sie im frühen Quantus-Netz handhabbar, wo Speicher noch kein Engpass ist, und Optimierungen wie Wormhole-Adressen mittels Zero-Knowledge-Beweisen werden das Skalieren adressieren.

Technische Implementierungsdetails siehe QIP-0006.

libp2p – quantensicheres netzwerk

Quantus Network sichert Peer-to-Peer-Kommunikation (P2P) durch Kombination von ML-DSA zur Authentifizierung und **ML-KEM** (Module-Lattice-Based Key-Encapsulation Mechanism, zuvor CRYSTALS-Kyber) zur Verschlüsselung. Diese Integration erweitert PQC auf den libp2p-Stack und modifiziert Kernkomponenten für Quantenresistenz: ML-DSA-87-Signaturen für Peer-Identität und ML-KEM-768 für Transportsicherheit (Erweiterung des Noise-Handshakes um eine zusätzliche KEM-Nachricht für quantenresistente gemeinsame Geheimnisse). [5]

Die P2P-Schicht wird in Quanten-Sicherheitsanalysen oft vernachlässigt. Peer-Authentifizierung ist wichtig, aber das Schlimmste, was ein Angreifer auf P2P-Ebene tun kann, ist einen

Knoten zu imitieren und ungültige Nachrichten zu senden, was Denial-of-Service verursachen könnte. Dieser Angriff wird bereits gemildert, weil Knoten im Blockchain-Modell in der Regel nicht vertrauenswürdig sind und bei Erkennung leicht den Schlüssel wechseln können. Ebenso bietet das Entschlüsseln von P2P-Kommunikation dem Angreifer begrenzte Vorteile (z. B. Transaktionspfade verfolgen, mit Proxies oder Tor milderbar), und die meisten Daten werden öffentlich auf der Kette sichtbar.

Dennoch schützt die quantensichere Absicherung der P2P-Schicht vor Abhören, Man-in-the-Middle-Angriffen und Quanten-Entschlüsselung und stellt sicher, dass Node-Gossip, Blockpropagation und andere Netzwerkinteraktionen in absehbarer Zeit vertraulich und integer bleiben.

Technische Details siehe QIP-0004.

pqc-skalierung – wormhole-adressen

Um die der Post-Quanten-Kryptographie innewohnenden Skalierungsherausforderungen anzugehen, führt Quantus Network ein innovatives aggregiertes Post-Quanten-Signaturschema namens **„Wormhole Addresses“** ein. Dieses System nutzt Zero-Knowledge-Beweise (ZKP), erzeugt mit dem Beweissystem Plonky2 (im Wesentlichen STARKs), um Saldo-Verifikation off-chain zu verlagern, sodass die Kette einen einzigen kompakten Beweis verifizieren kann, ohne einzelne Signaturen zu verarbeiten. Wormhole Addresses ermöglichen die Verifikation vieler

Transaktionen mit einem Beweis; die öffentlichen Inputs (z. B. Nullifiers, Speicher-Root, Ausgangsadressen und Beträge) sind der Haupt- Engpass. Dadurch sinken die amortisierten Speicheranforderungen pro Transaktion auf etwa 256 zusätzliche Bytes pro Transaktion, weit unter jedem bekannten PQC-Signaturschema.

Die Quantensicherheit des Schemas kommt vom Einsatz der sicheren Hashfunktion **Poseidon2** für Commitments über FRI (Fast Reed-Solomon Interactive Oracle Proofs) statt der in SNARKs üblichen, quantenverwundbaren Elliptische-Kurven-Paarungen.

Außerdem bleiben Authentifizierungsgeheimnisse hinter Poseidon2 verborgen. Da sichere Hashfunktionen durch Grovers Algorithmus nur quadratisch geschwächt werden, brechen sie nicht; Hash-Preimage-Beweise können als leichte Post-Quanten-Signaturen in ZK-Kontexten dienen, ähnlich hashbasierten Schemata wie SPHINCS+.

client-/prover-flow

Nutzer erzeugen eine nachweislich nicht ausgebende Adresse durch doppeltes Hashen eines Salzes zusammen mit einem Geheimnis:

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

Diese Konstruktion vermeidet Fehlalarme (z. B. Verwechslung einer einfachen Hash-Public-Key mit einer nicht ausgebenden Adresse), weil in Substrate (und allgemein) Blockchain-Adressen der einfache Hash eines aus dem privaten Schlüssel algebraisch abgeleiteten öffentlichen Schlüssels sind, nicht ein sicherer Hash. Die Sicherheit der Konstruktion reduziert sich damit auf das Finden der Preimage-zur-Preimage eines sicheren Hashs. An diese Adresse gesendete Tokens werden faktisch verbrannt. Sie können nicht ausgegeben werden, weil es keinen privaten Schlüssel für die empfangende Adresse gibt. Diese Coins können neu geprägt werden, ohne das Angebot zu inflieren.

Für jede Übertragung wird ein Speicherobjekt TransferProof erstellt, mit Details wie einer global eindeutigen Transferanzahl. Das Nutzer-Wallet erzeugt einen Merkle-Patricia-Trie (MPT)-Speicherbeweis von der Speicher-Root eines aktuellen Block-Headers bis zum Blatt dieses TransferProof. Ein Nullifier wird berechnet, um Doppelausgaben zu verhindern:

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

aggregator-flow

Jede Partei (Client, Miner oder Dritte) kann mehrere Beweise mittels Plonky2-Rekursion aggregieren und einen Beweisbaum bilden, in dem jeder Elternbeweis die Kinder verifiziert und die öffentlichen Kind-Inputs aggregiert:

— Nullifiers passieren unverändert

— Ausgangsadressen werden dedupliziert

— Block-Hashes werden verknüpft nachgewiesen und dann bis auf den neuesten verworfen

— Beträge für doppelte Ausgangsadressen werden summiert

chain-/verifier-flow

Das Netzwerk verifiziert den aggregierten Beweis durch Prüfung: Block-Hash ist in der Kette und aktuell, Eindeutigkeit des Nullifiers (gegen Doppelausgabe) und Gültigkeit des Beweises. Der ZK-Schaltkreis erzwingt Korrektheit des Speicherbeweises, Genauigkeit des Nullifiers, Nicht-Ausgebbarkeit der Adresse, Übereinstimmung der Salden zwischen Ein- und Ausgängen und Verkettung der Block-Header.

warum plonky2

— Bereits auditiert

— Post-quantenfest

— Ohne trusted setup

— Effizientes Beweisen/Verifizieren

— Flüssige Beweisaggregation

— Native Rust-Implementierung

— Kompatibel mit Substrates no-std-Umgebung

LEISTUNG

Rekursive Beweise enden in 170 Millisekunden mit kompakten Größen (100 KB pro aggregiertem Beweis). Im optimalen Fall mit 5-MB-Blöcken und allen Transaktionen zur gleichen Ausgabe könnten Wormhole Addresses ~153.000 Transaktionen in einem Block bündeln (4,9 MB / 32 Bytes pro Nullifier): eine Verbesserung um den Faktor 223 gegenüber ~685 rohen ML-DSA-Transaktionen (5 MB / 7,3 KB je Transaktion).

sicherheitshinweise

Potenzielle Risiken umfassen Inflationsfehler durch fehlerhafte Schaltkreis-/Verifikationsimplementierungen, die jedoch wirtschaftlich erkennbar wären, wenn neu geprägte Coins die Salden von Null-Sende-Adressen übersteigen. Nutzer können optional nachweisen, dass eine Adresse eine Wormhole-Adresse ist, indem sie den ersten Hash ohne Offenlegung des Geheimnisses veröffentlichen. Verifikationstransaktionen sind nicht signiert, daher muss DoS durch fehlgeschlagene Transaktionen ohne finanzielle Mittel gemildert werden. Token-Supply-Berechnungen bleiben konsistent, da Neu-Prägungen als neue Coins erscheinen, aber durch Verbrennungen maximale Supply-Garantien erhalten.

Weitere technische Details siehe QIP-0005.

konsensmechanismus

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

Wichtig: Diese Änderung erfolgt nicht wegen Quantensicherheit. Kryptographische Hashfunktionen wie SHA-256 werden durch Quantenalgorithmen, insbesondere Grover, geschwächt, aber nicht zerstört. Einige Post-Quanten-Signaturschemata nutzen aus diesem Grund sichere Hashes als Grundbaustein.

Poseidon2 ist eine Verfeinerung der Hashfunktion Poseidon. SNARKs oder STARKs für Berechnungen mit traditionellen Hashes wie SHA-256 zu erstellen erfordert typischerweise fast 100-mal mehr Gatter als mit Poseidon, das vollständig auf algebraischen Feldoperationen statt Bitoperationen beruht.

Wir verwenden das **Goldilocks-Feld** für Poseidon2 und Plonky2. Die Ordnung des Goldilocks-Feldes passt in eine 64-Bit-Unsigned-Integer, was die Effizienz erhöht, ohne die Solidität zu gefährden.

05

vermögenserhalt

Beim Umgang mit Kryptowährungsschlüsseln gibt es viele Risiken. Die meisten lassen sich vermeiden.

umkehrbare transaktionen

Quantus Network bietet nutzerkonfigurierbare umkehrbare Transaktionen. Absender legen ein Zeitfenster fest, in dem sie ausgehende Überweisungen stornieren können. Das erschwert Diebstahl und korrigiert Fehler, ohne die Finalität zu opfern. Das System nutzt ein modifiziertes Substrate-„Scheduler“-Pallet mit Zeitstempeln. Wallets zeigen Countdowns für Absender (mit Stornieren-Button) und Empfänger.

Umkehrbare Transaktionen ermöglichen neuartige Sicherheitsprotokolle bei dezentraler Anwendung on-chain.

Weitere technische Details siehe QIP-0009.

prüfsätze

Quantus Network führt „Check-Phrases“ ein – eine lesbare, kryptographisch sichere Prüfsumme für Blockchain-Adressen. Die Adresse wird gehasht, um eine kurze Folge merkbarer Wörter aus der BIP-39-Mnemonik-Liste zu erzeugen. Prüfsätze schützen vor Tippfehlern, Manipulation und Address-Poisoning-Angriffen. Eine

Schlüsselableitungsfunktion mit 50.000 Iterationen macht Rainbow-Table-Angriffe teuer. Bei großen Transaktionen sollten Nutzer weiterhin jedes Zeichen der Adresse prüfen.

Weitere technische Details siehe QIP-0008.

hochsicherheitskonten

Jedes Konto kann zu einem „Hochsicherheitskonto“ mit verpflichtenden Revertierungsperioden für alle ausgehenden Überweisungen aufgewertet werden. Ein benannter **Guardian** (Hardware-Wallet, Multisig oder vertrauenswürdige Dritte) kann verdächtige Transaktionen während der Revertierungsperiode stornieren und Mittel an den Guardian statt an Absender oder Empfänger senden. Diese Opt-in-Funktion ist nach Aktivierung dauerhaft und verhindert, dass Diebe sie deaktivieren.

Guardians können verkettet werden: Der Guardian eines Hochsicherheitskontos kann selbst ein Hochsicherheitskonto mit eigenem Guardian sein. So entstehen komponierbare Hierarchien, in der jeder Guardian höhere Befugnisse über das geschützte Konto hat. Das Design gibt Nutzern Zeit, unbefugte Aktivität zu erkennen und zu reagieren, ohne die Finalität legitimer Überweisungen zu gefährden.

Weitere technische Details siehe QIP-0011.

schlüsselwiederherstellung

Viele Krypto-Vermögen sind mit ihren Besitzern ins Grab gegangen. Quantus Network bietet eine einfache Möglichkeit, eine Wiederherstellungsadresse anzugeben, die jederzeit Mittel abheben kann, vorbehaltlich einer festen Verzögerung. In dieser Zeit kann der Eigentümer die Wiederherstellung ablehnen, wenn er noch Zugriff auf den Schlüssel hat. Diese Funktion ermöglicht Überleben: Nutzer haben ein On-Chain-Testament ohne Gerichte oder formale Erbfolge.

hd-lattice

Hierarchisch-deterministische (HD) Wallets sind der Branchenstandard für Blockchains und erlauben, eine einzige Seed-Phrase für alle Schlüssel zu sichern – mit besserer Sicherheit und Komfort gegenüber manuellen Kopien pro Aktion. Die Übertragung auf Gitterschemata wie Dilithium wirft zwei Herausforderungen auf:

— HMAC-SHA512-Ausgaben können nicht direkt private Gitterschlüssel bilden, die Polynome aus einem Ring mit bestimmten Eigenschaften sind.

— Nicht gehärtete Schlüsselableitung beruht auf Elliptische-Kurven-Addition, die in Gittern fehlt (öffentliche Schlüssel sind unter keiner algebraischen Operation abgeschlossen).

Quantus Network löst den ersten Punkt, indem die HMAC-Ausgabe als Entropie dient, um den privaten Schlüssel deterministisch zu

konstruieren, nicht als den Schlüssel selbst. Der zweite Punkt ist weniger kritisch und bleibt eine offene Forschungsfrage, ob sich Gitter-Kryptographie so anpassen lässt, dass er gelöst wird.

Weitere technische Details siehe QIP-0002.

06

tokenomics und governance

Quantus Network operiert in einem sich wandelnden Umfeld; wir können nicht davon ausgehen, beim ersten Versuch alles richtig zu machen. Daher wählen wir einen einfachen Ausgangspunkt und erlauben dem Governance-System, Änderungen vorzunehmen, sobald neue Erkenntnisse vorliegen. Dieses Design macht die Blockchain zu einer lebendigen Entität, die sich an ihre Umgebung anpassen kann. Insbesondere erlaubt der Substrate-Governance-Prozess tiefgreifende On-Chain-Änderungen mit minimaler Koordination zwischen den verschiedenen Knotenbetreibern.

blockbelohnungen

Quantus Network nutzt ein einfaches Tokenomics-Modell nach Bitcoin-Vorbild. Es gibt ein maximales Angebot von **21.000.000 Coins** und eine einfache Heuristik bestimmt die Blockbelohnung:

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

Diese Heuristik bildet eine sanft fallende Exponentialkurve, während die block_reward zum current_supply beiträgt und damit die im nächsten Block berechnete block_reward senkt. Gebühren- und andere Verbrennungen reduzieren das current_supply und werden Teil des Blockbelohnungsbudgets. Die Konstante ist so

gewählt, dass ohne jegliche Verbrennung etwa 99 % der Coins in etwa 30 Jahren ausgegeben werden.

zuordnung an investoren

Quantus Network wurde mit Hilfe von Investoren aufgebaut, die hohes Risiko bei der Finanzierung trugen. Private Investoren unterliegen einem 4-Jahres-Vesting, wie das Team. Investoren aus dem öffentlichen Verkauf erhalten am ersten Tag volle Liquidität. Die im öffentlichen Verkauf eingenommenen Mittel werden mit Tokens gepaart und für Liquidität (DEX, CEX und Market Maker) verwendet. Diese Investorenzuordnungen zusammen mit der Liquidität bilden den einzigen „Pre-Mine“. Der Rest der Tokens muss geschürft werden, bis das volle Angebot erreicht ist.

Wird weniger als das Maximum von 10 % während des öffentlichen Verkaufs verkauft, erfolgt eine proportionale Reduktion der Liquiditäts-Tokens und der Rest wird Minern über Blockbelohnungen ausgegeben.

zuordnung an das unternehmen

Um das Team für das Risiko des Aufbaus neuer Technologie ohne Erfolgsgarantie zu entschädigen, geht ein Teil der Blockbelohnung über etwa vier Jahre an das Unternehmen. Das entspricht faktisch einem Vesting von etwa **15 % des Gesamtangebots** für das Unternehmen.

Danach kann der Unternehmensanteil an Blockbelohnungen abgeschaltet, angepasst oder per Token-Inhaber-Vote umgeleitet werden.

transaktionsgebühren

TRANSAKTIONSTYP	GEBÜHRENSTRUKTUR	ZIEL
Standard	Feste Gebühr	Miner
Umkehrbar (Hochsicherheit)	1 % auf Volumen	Verbrennu
ZK-aggregiert	0,1 % auf Volumen	50 % Mine / 50 % Verbrennu

fork-freie upgrades

Quantus Network unterstützt „fork-freie“ Upgrades über Substrate-Runtime-Upgrades, sodass die Kern-Blockchain-Logik (die „Runtime“) ohne störende Hard Forks oder Spaltung der Community evolvieren kann. Das gelingt durch On-Chain-Governance-Referenden, bei denen genehmigte Vorschläge einen Runtime-Swap auslösen – im Wesentlichen wird der bestehende WASM-Code-Blob in einem einzigen Block durch einen neuen ersetzt, mit Erhalt von Zustand und Betrieb. Dieser Weg minimiert Ausfallzeiten und Risiken und ermächtigt die Community, das

Protokoll iterativ zu verfeinern, wenn der echte Nutzungsfall Verbesserungen zeigt.

Wenn die Community Vertrauen ins System gewinnt, wird die Macht, die Runtime zu ändern, deutlich reduziert, um die Angriffsfläche zu begrenzen, falls ein böswilliger Akteur die Kontrolle über den Upgrade-Prozess erlangt.

governance-system

Quantus Network übernimmt sein Governance-Rahmenwerk vom OpenGov-System von Polkadot über Substrate. Token-Inhaber nehmen per **Conviction Voting** teil und sperren ihre Assets für unterschiedlich lange Zeiträume, um das Stimmgewicht zu verstärken. Die Verstärkung reicht von 1× (ohne Sperre) bis 6× (maximale Sperre). Dieses Design fördert langfristige Ausrichtung, indem Einfluss an Commitment gebunden wird.

Vorschläge werden in mehrere Abstimmungsspuren („Origins“) eingeteilt. Jeder Origin hat maßgeschneiderte Parameter wie Zustimmungsschwellen (z. B. qualifizierte Mehrheit für hochimpactige Änderungen), Mindestdepots gegen Spam, Vorbereitungs-/Ausführungsperioden und Entscheidungsfristen gegen Blockaden. Dieses Mehrspur-Design erlaubt parallele Referenden – von routinemäßigen Treasury-Ausgaben bis zu kritischen Runtime-Upgrades.

Das **Technical Collective** ist eine kuratierte Gruppe technischer Expertinnen und Experten, die als Spezialorgan für dringende technische Angelegenheiten vorschlägt, prüft oder whitelistet und sie über eine dedizierte Spur beschleunigt, bei gemeinschaftlicher Aufsicht.

Quantus übernimmt dieses System unverändert, startet aber mit einer minimalen Konfiguration, um früh Komplexität zu vermeiden. Zunächst ist nur die Spur des Technical Collective aktiv, genutzt für verbindliche Hochprivileg-Entscheidungen wie Protokoll-Upgrades oder Parameteranpassungen.

Später kann Quantus eine nicht verbindliche Community-Abstimmungsspur hinzufügen, um Stimmungen zu nicht durchsetzbaren Themen zu erfassen, etwa Feature-Vorschläge oder Ökosystem-Umfragen. Dieses System wird verbindlich, wenn das Unternehmen das Netz an die DAO übergibt. Dieser phasenweise Ansatz erlaubt organisches Wachstum des Netzes durch künftige Governance-Votes, ohne Nutzer am Anfang mit unnötiger Komplexität zu belasten.

07

roadmap

Die aktuelle Roadmap bis 2026, vorbehaltlich Änderungen.

heisenberg inception Dezember 2024	Finanzierung gesichert, Substrate gewählt.
resonance alpha Juli 2025	Öffentliches Testnet, Dilithium-Signaturen, umkehrbare Transaktionen.
schrödinger beta Oktober 2025	Vollständige Features, bereit für Audit.
dirac beta November 2025	PoW auf Poseidon2 umgestellt, Audits adressiert.
planck beta Januar 2026	Hochsicherheitskonten, Multisig, Hardware-Wallet, ZK-Integration.
bell mainnet Q2 2026	Mainnet-Start.
fermi upgrade Q4 2026	Infrastruktur für ZK-Beweisaggregation.

08

risiken

Den Aufbau von Quantus Network begleiten inhärente Risiken.

implementierungsprobleme

Fehler in der Softwarelogik können selbst in den besten designten Systemen schwere Ausfälle verursachen.

probleme bei der nist-algorithmenauswahl

Potenzielle Fehler oder Hintertüren in ausgewählten Post-Quanten-Standards (z. B. ML-DSA, ML-KEM), die nach der Standardisierung auftauchen könnten. Im schlimmsten Fall würden solche Fehler es einem Angreifer erlauben, Signaturen zu fälschen, indem er den privaten aus dem öffentlichen Schlüssel ableitet – ein katastrophaler Kettenfehlmodus. Wenn solche Fehler öffentlich werden, könnte Quantus Network auf einen neuen Algorithmus upgraden, doch bei seltener Ausnutzung werden sie vielleicht nie entdeckt.

zeitrahmen des quantencomputings

Quantenfortschritte könnten viel später kommen als erwartet und die PQC-Notwendigkeit verzögern; umgekehrt könnte geheime Entwicklung (z. B. durch Regierungen) plötzliche Bedrohungen

erzeugen, wenn die Blockchain-Community nicht schnell genug upgraded.

sonstige überlegungen

Allgemeine Adoptionsbarrieren, regulatorische Unsicherheit in Finanzen/Blockchain und die inhärente Volatilität von Krypto-Ökosystemen.

09

referenzen und weiterführende literatur

[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