Quantus Network Whitepaper

Authors: Christopher Smith | **Last updated:** January 14, 2026

Introduction

The Quantum Threat

Traditional blockchains face an existential threat from the advent of quantum computing. The cryptographic foundations of blockchains rely on the hardness of the discrete logarithm problem (DLP), and quantum algorithms, notably Shor's, can solve the DLP exponentially faster than classical computers. This vulnerability could enable quantum-adversaries to derive private keys from public keys, which would allow them to forge transactions and decrypt sensitive financial data.

The outcome is a catastrophic system failure. Without proactive quantum-resistant upgrades, the trillion-dollar crypto economy risks sudden devaluation from such attacks.

> 💡 TIP
>
> **Quantus fixes this.**

Unique Value Proposition

Named after the Latin word for "how much", Quantus Network delivers scalable, quantum-secure wealth preservation. Quantus is not a smart contract platform. Instead, like a high-end restaurant with no menu, Quantus is focused on doing a small number of things better than any other chain.

Specifically, Quantus uses:

- Post-quantum signatures for all transactions
- Post-quantum signatures and encryption (ML-DSA and ML-KEM) to secure peer connections
- A post-quantum bridge to other blockchains and create quantum-secure wrapped coins

- Post-quantum zero-knowledge-proofs to scale
- High Security Accounts to deter theft and enable recovery from mistakes
- Human-readable check-phrases for easy address verification

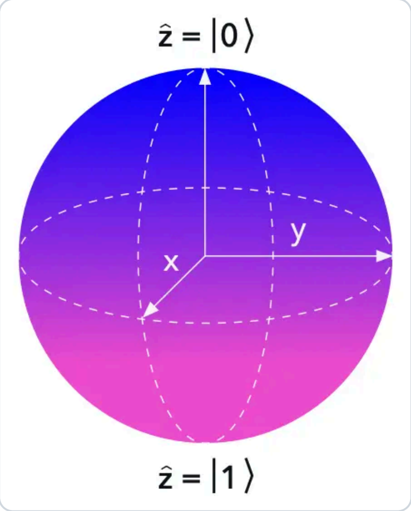
This targeted approach empowers users to preserve wealth confidently, turning quantum threats into opportunities.

> 💡 **TIP**
>
> Quantus is the future-proof fortress for your fortune.

The Quantum Threat to Blockchain

Quantum Computing Basics

Quantum computers leverage principles like superposition and entanglement to perform computations that are intractable for classical machines.



Unlike classical bits, which are either 0 or 1, quantum bits (qubits) can exist in multiple states simultaneously, enabling exponential parallelism for certain problems. **This capability poses existential risks to the cryptographic systems underpinning blockchain finance, as algorithms developed for quantum hardware undermine the security assumptions of most public-key cryptography**.

Shor's Algorithm

Introduced in 1994 by Peter Shor, provides a polynomial-time method for factoring large integers and solving the discrete logarithm problem on a quantum computer. In essence, it exploits Quantum Fourier Transforms (QFT) to find the period of a function, allowing efficient reversal of the trapdoor functions that underlie schemes like RSA or elliptic curve cryptography (ECC).

For blockchain finance, this means an attacker with a sufficiently powerful quantum computer (estimated at ~2,300 logical qubits) could derive private keys from public keys in polynomial time $O(n^3)$. This is an extreme speed-up, rendering vulnerable systems obsolete overnight.

Grover's Algorithm

Proposed by Lov Grover in 1996, offers a quadratic speedup for unstructured search problems, reducing the time to find a specific item in an unsorted database from O(n) to O(√n) operations. It works by iteratively amplifying the amplitude of the target state through quantum interference. While not as devastating as Shor's for asymmetric cryptography, **Grover's impacts symmetric primitives like hash functions and AES encryption, effectively halving the security level** (e.g., a 256-bit key behaves like 128 bits against quantum attacks).

While impactful, this attack is mitigated by simply doubling the security bits, rather than changing the cryptographic scheme. Additionally, Grover's quadratic speedup is impractical due to its high qubit and gate requirements, requiring billions of operations in sequence, with limited parallelization, making it infeasible for real-world reversals even on future hardware.

The dangers of quantum computing to blockchain finance can be categorized into four areas:

Forging Digital Signatures

Shor's algorithm directly threatens ECC-based signatures used in most blockchains (e.g., Bitcoin's secp256k1 curve), allowing adversaries to impersonate users and authorize fraudulent transactions. Such a capability would represent a critical failure of the most basic feature of a blockchain.

Forging False Proofs in Zero-Knowledge Systems

Many zero-knowledge proofs, such as those in zk-SNARKs for privacy- focused finance, rely on discrete logarithm hardness via elliptic-curve pairings for commitments; Shor's could enable the creation of invalid proofs that appear valid, which could allow an attacker to mint new coins or falsify the state of Layer-2s (L2s).

Decrypting Secret Information

Quantum attacks could expose encrypted data protected by vulnerable public-key schemes in privacy protocols such as Zcash or Monero. It could also decrypt p2p communications in financial protocols, revealing sensitive wealth details and enabling targeted theft.

Reversing Hash Functions

Grover's algorithm could accelerate preimage attacks on hashes like SHA-256, used for proof-of-work and address generation, but this is the least concerning threat. Many post-quantum cryptographic schemes incorporate hash-based constructions as hashes are considered secure- enough with a large enough digest.

Scaling Challenges in Post-Quantum Cryptography

While post-quantum cryptography (PQC) offers essential protections against quantum threats, it introduces significant scaling hurdles due to the inherent design of these algorithms. Unlike elliptic curve schemes, which rely on compact mathematical structures, PQC primitives require larger parameters to maintain security against both classical and quantum adversaries. This results in substantially bigger public keys, private keys, and signatures, often by orders of magnitude.

The following table illustrates typical sizes for ML-DSA at a 128-bit post-quantum security level compared to classical counterparts like 256-bit ECDSA:

Algorithm	Public Key Size (Bytes)	Private Key Size (Bytes)	Signature Size (Bytes)
ML-DSA-87 (Dilithium)	2,592	4,896	4,627
ECDSA (256-bit)	32	32	65

As shown, ML-DSA signatures can be over 70 times larger than ECDSA equivalents, and public keys more than 80 times larger.

Other PQC families exacerbate this: hash-based schemes like SPHINCS+ may produce signatures up to 41 KB, while even size-optimized lattice variants like FALCON still exceed classical sizes by a significant multiple.

In blockchain contexts, these inflated sizes compound into systemic scaling issues. Larger signatures bloat individual transactions, reducing transactions per second (TPS) as blocks fill faster and require more time for validation. This also strains peer-to-peer (P2P) communication, increasing bandwidth demands and propagation delays, which can heighten the risk of network forks or orphaned blocks in consensus mechanisms like proof-of-work. Storage requirements are also affected, leading to higher node operating costs and barriers for participation, especially for resource-constrained users or validators.

These scaling challenges will have to be addressed by all blockchains in the future. Bitcoin, for example, will have much less than 1 TPS if the max block size is not increased.

Quantus Network Architecture

Post-Quantum Cryptographic Primitives

Quantus Network employs **NIST-standardized PQC** primitives to ensure the security of transactions and network communications against quantum threats. At the core of transaction integrity is **ML-DSA (Module-Lattice-based Digital Signature Algorithm**, formerly known as CRYSTALS-Dilithium), a lattice-based signature scheme selected for its balance of security, efficiency, and ease of implementation. **ML-DSA leverages the hardness of problems** like Learning With Errors (LWE) and Short Integer Solution (SIS) over module lattices, providing robust resistance to both classical and quantum attacks, including those from Shor's algorithm.

For transaction signatures, **Quantus integrates ML-DSA-87**, the parameter set offering the highest security level (NIST Security Level 5, equivalent to 256-bit classical and 128-bit quantum security) to **protect against potential cryptanalytic breakthroughs in lattice problems**. This choice prioritizes caution, as lattice cryptography is relatively new and less battle-tested than classical schemes. The larger parameters mitigate risks from potential advances in lattice cryptanalysis, which would still leave smaller key sizes as softer targets.

Alternatives

ML-DSA was selected over alternatives like FN-DSA (Falcon) due to:

- FN-DSA's greater implementation complexity (e.g., requiring floating-point operations, which are blockchain-unfriendly)
- Lack of deterministic key generation in its specification
- Its non-finalized status at the time of development

Hash-based options like SLH-DSA were dismissed for their even larger signature sizes (exceeding 17 KB). Crypto-agility (being able to swap in different signature schemes) is built into Substrate, so it is relatively easy to add these alternatives at a future date, should circumstances demand.

While ML-DSA-87 results in larger keys and signatures, these are manageable in Quantus's early-stage network, where storage is not yet a bottleneck, and future optimizations like wormhole addresses via zero-knowledge proofs will address scaling.

For technical details about the implementation see QIP-0006.

LibP2P

Quantus Network secures peer-to-peer (P2P) node communications using a combination of ML-DSA for authentication and ML-KEM (Module-Lattice-based Key Encapsulation Mechanism, formerly CRYSTALS-Kyber) for encryption.

This integration extends PQC to the libp2p networking stack, modifying core components for quantum resistance: using ML-DSA-87 signatures for peer identity and ML-KEM-768 for transport security (extending the Noise handshake with an additional KEM message for quantum-resistant shared secrets).

The P2P layer is often neglected in quantum-security analysis. Authentication of peers is important, but the worst an attacker could do at the peer level is impersonate a node and send invalid messages, which could result in denial-of- service. This attack is already mitigated by the fact that nodes are generally untrusted in the blockchain model and nodes can easily switch their keys if the attack is detected. Likewise, decrypting P2P communications yields limited attacker benefits (e.g., tracking transaction paths, mitigated by proxies or Tor), and most data becomes public on-chain anyway.

Nevertheless, quantum-securing the P2P layer protects against eavesdropping, man-in-the-middle attacks, and quantum decryption, ensuring that node gossip, block propagation, and other network interactions remain confidential and tamper-proof for the foreseeable future.

For technical details about the implementation see QIP-0004.

Scaling PQC

To address the scaling challenges inherent in post-quantum cryptography, **Quantus Network introduces an innovative aggregated post-quantum signature scheme called "Wormhole Addresses".** This system leverages zero-knowledge proofs (ZKPs) generated via the Plonky2 proving system (basically STARKs) to move balance verification off-chain, allowing the chain to verify a single compact proof without processing individual signatures.

Wormhole Addresses enable the verification of a large number of transactions with one proof, with the public inputs (e.g., nullifiers, storage root, exit addresses, and amounts) becoming the primary limiting factor. This reduces the amortized per-transaction storage demands to **approximately 256 additional bytes per transaction, much smaller than any known PQC signature scheme.**

The quantum security of the scheme derives from the use of the secure hash function Poseidon2 for commitments via FRI (Fast Reed-Solomon Interactive Oracle Proofs), instead of the quantum-vulnerable elliptic-curve pairings commonly used in SNARKs.

Additionally the authentication secrets are hidden behind Poseidon2. Since secure hash functions are only quadratically weakened by Grover's algorithm, not broken, hash preimage proofs can serve as lightweight post-quantum signatures in ZK contexts, similar to hash-based schemes like SPHINCS+.

Client / Prover Flow

Users generate a provably unspendable address by double-hashing a salt concatenated with a secret:

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

This construction prevents false positives (e.g., mistaking a single-hash public key for an unspendable address) because in Substrate (and generally) blockchain addresses are the single hash of a public key, which is derived from the private key via some algebraic operation, not via a secure hash. The security of the construction therefore reduces to finding the preimage-of-a-preimage of a secure hash. Tokens sent to this address are effectively burned. They cannot be spent because no private key exists for the address that received them. These coins can therefore be re-minted without inflating supply.

For each transfer, a TransferProof storage object is created, containing details like a unique global transfer count. The user's wallet generates a Merkle-Patricia-Trie (MPT) storage proof from a recent block header's storage root to the leaf for this TransferProof.

A nullifier is computed:

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

To prevent double-spends, with the secret derived deterministically from the wallet seed for retention.

Aggregator Flow

Any party (client, miner, or third-party) can aggregate multiple proofs using Plonky2's recursion, forming a tree of proofs where each parent proof is a verification of the child proofs, with the child proofs' public inputs aggregated:

- nullifiers pass unchanged
- exit addresses are deduplicated
- block hashes are proven to be linked and then all but the most recent is dropped
- amounts for duplicate exit addresses are summed This recursion supports hierarchical aggregation, drastically reducing on-chain data.

Chain / Verifier Flow

The network verifies the aggregated proof by checking:

- block hash is on chain and recent
- nullifier uniqueness (to prevent double-spends)
- proof validity

The ZK circuit enforces:

- storage proof correctness
- nullifier computation accuracy
- address unspendability
- balance match between inputs and outputs
- block header linkage

Plonky2 was selected for the following reasons:

- already audited
- post-quantum
- no trusted setup
- efficient proving/verification
- seamless proof aggregation
- Rust-native implementation
- compatible with Substrate's no-std environment

Performance highlights include:

Recursive proofs in 170 milliseconds and compact sizes (100 KB per aggregated proof), enabling massive throughput gains.

In an optimal case with 5 MB blocks and all transactions going to the same output, **Wormhole Addresses could pack ~153,000 transactions into a single block** (4.9 MB / 32 bytes per nullifier), a 223x improvement over ~685 raw ML-DSA transactions (5 MB / 7.3 KB each).

Security Notes

Potential risks include inflation bugs from faulty circuit/verification implementations, although this would be economically detectable if re-minted coins exceed balances of zero-send addresses. Users can optionally prove an address is a wormhole by publishing the first hash without revealing the secret. Verification transactions are unsigned, so denial-of-service via failed transactions needs to be mitigated non- financially. Token supply calculations are maintained, as re-mints appear as new coins but maintain maximum supply guarantees via burns.

For more technical details about the implementation see QIP-0005.

Consensus Mechanism

Quantus Network uses a Proof-of-Work (PoW) consensus algorithm that preserves the desirable properties of Bitcoin's consensus algorithm while improving compatibility with ZK-proof systems by switching out SHA-256 with Poseidon2.

Importantly, this change is not being made for quantum security. Cryptographic hash functions like SHA-256 are weakened but not destroyed by quantum algorithms, notably Grover's. Some post-quantum signature schemes use secure hashes as a building block for this reason.

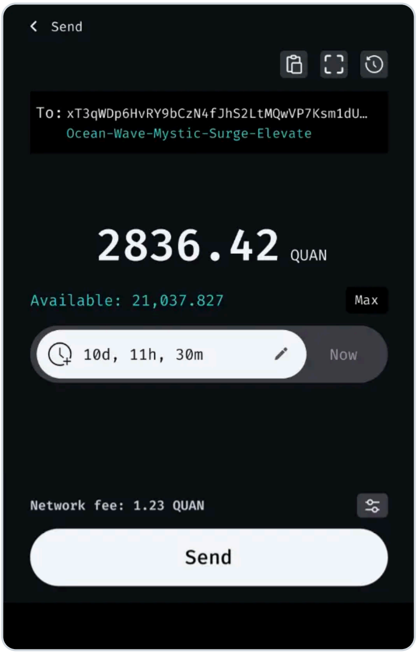
Poseidon2 is a refinement of the Poseidon hash function. Creating SNARKs or STARKs for computations involving traditional hash functions like SHA-256 often requires nearly 100x the number of gates compared to using Poseidon, which relies entirely on algebraic functions over field elements, instead of bit- level operations. We use the Goldilocks field for both Poseidon2 and Plonky2 to maximize the efficiency.

Wealth Preservation

There are many risks in managing cryptocurrency keys. Most of them are avoidable. Quantus Network bakes ease-of-use into the chain itself, enabling non-experts to transact with peace-of-mind.

Reversible Transactions

Quantus Network offers user-configurable reversible transactions, enabling senders to set a time window during which they can cancel outgoing transfers, enhancing theft deterrence and error correction without sacrificing blockchain's core irreversibility. Leveraging a modified Substrate "scheduler pallet" that uses timestamps for intuitive delays, the system allows clients to schedule transfers via a simple interface, displaying countdowns in wallets for both sender (with a cancel button) and recipient (indicating completion if not cancelled). This balances quick finality for commerce with flexibility for users concerned about making mistakes or wanting to make a good faith deposit without an escrow service.



To: xT3qWDp6HvRY9bCzN4fJhS2LtMQwVP7Ksm1dU…
Ocean-Wave-Mystic-Surge-Elevate

2836.42 QUAN

Available: 21,037.827

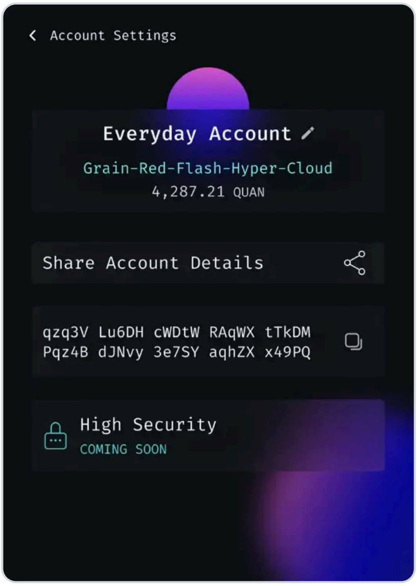
10d, 11h, 30m

Network fee: 1.23 QUAN

Reversible transactions form a powerful building block for novel security protocols while maintaining decentralization through on-chain enforcement.

For more technical details see QIP-0009.

Check-Phrases



< Account Settings

Everyday Account

Grain-Red-Flash-Hyper-Cloud

4,287.21 QUAN

Share Account Details

qzq3V Lu6DH cWDtW RAqWX tTkDM Pqz4B dJNvy 3e7SY aqhZX x49PQ

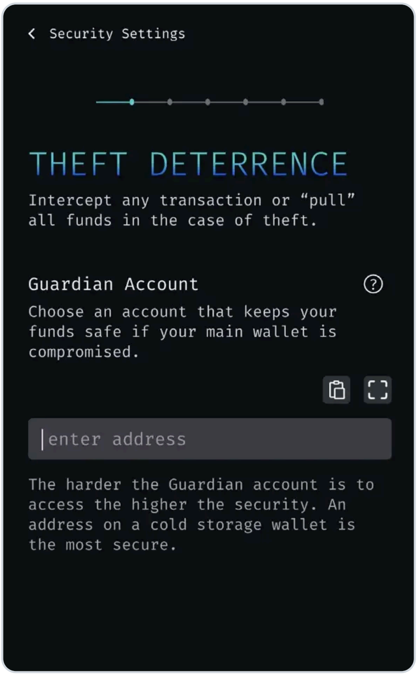
High Security

COMING SOON

Quantus Network introduces “check-phrases,” a cryptographically-secure human-readable checksum for blockchain addresses and other data requiring human verification. **By hashing the address to generate a short sequence of memorable words from the BIP-39 mnemonic list, check-phrases enable quick, error-proof integrity checks, protecting against typos, tampering, and attacks like address poisoning**. This tool allows users to confidently verify addresses during transfers without relying on truncated displays or weak checksums. A 50,000 iteration key derivation function is used to ensure that creating a rainbow table for given checksums is very expensive. Of course, for large transactions, users should still manually check every letter of the address for correctness.

For more technical detail please see QIP-0008.

High-Security Accounts



Security Settings

THEFT DETERRENCE

Intercept any transaction or “pull” all funds in the case of theft.

Guardian Account

Choose an account that keeps your funds safe if your main wallet is compromised.

enter address

The harder the Guardian account is to access the higher the security. An address on a cold storage wallet is the most secure.

Quantus Network offers the ability to upgrade any account to a “high-security account” which enforces mandatory reversal periods on all outgoing transfers, allowing a designated “guardian” account such as a hardware wallet, multisig, or even a user-chosen trusted-third-party to exclusively cancel suspicious transactions during the reversal period, sending the funds to the guardian instead of the sender or receiver. This opt-in, permanent feature builds on reversible transfers, where users specify the delay and interceptor upon activation, preventing thieves from disabling it.

The interceptor can itself be another high-security account with its own guardian, enabling composable hierarchies where each guardian has superior permissions to the account it protects. This design mimics traditional finance’s court-ordered reversals but with user control. It balances security and convenience for high-value accounts, giving time to detect and respond to unauthorized activity without compromising blockchain finality for legitimate flows.

For more technical details see QIP-0011.

Key Recovery

Many crypto-fortunes have gone to the grave with their owners. Quantus Network offers a simple way to specify a recovery address that can pull your funds at any time, subject to a fixed delay. During this time, the owner can deny recovery if they have access to the key. This feature enables survivorship: users have an on-chain will without the need for courts or estates.

HD-Lattice

Hierarchical Deterministic (HD) wallets are the industry standard for blockchains, allowing users to back up one seed phrase for all keys, improving security and convenience over manual backups per action.

Adapting this to lattice schemes like Dilithium involves two challenges:

- HMAC-SHA512 outputs can’t directly form lattice private keys, which require “good basis” polynomials via rejection sampling.
- Non-hardened key derivation relies on elliptic curve addition, absent in lattices (public keys aren’t closed under any algebraic operation).

Quantus Network addresses the first issue by using the output of the HMAC as entropy to deterministically construct the private key, not as the private key itself. The second issue is less critical and remains an open research question whether lattice cryptography can be adapted to address it.

For more technical details see QIP-0002.

Tokenomics and Governance

Quantus Network exists in a changing environment, and we cannot assume that we will get everything right on the first try. For this reason, we choose a simple starting point and allow the governance system to make changes as new information is acquired. This design makes the blockchain a living entity that can adapt to its environment at will. In particular, the Substrate governance process allows deep changes to the chain with minimal coordination among the various node-runners.

Block Rewards

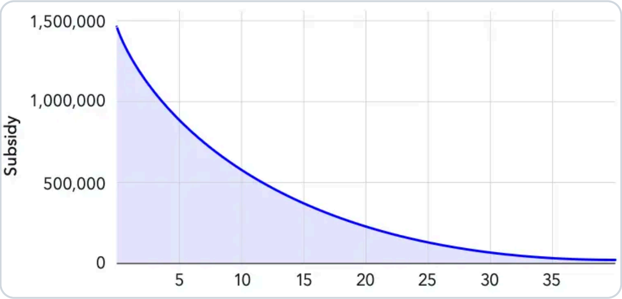
Quantus Network employs a straightforward tokenomics model imitating that of Bitcoin. There is a maximum supply of 21,000,000 coins and a simple heuristic determines the reward each block.

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

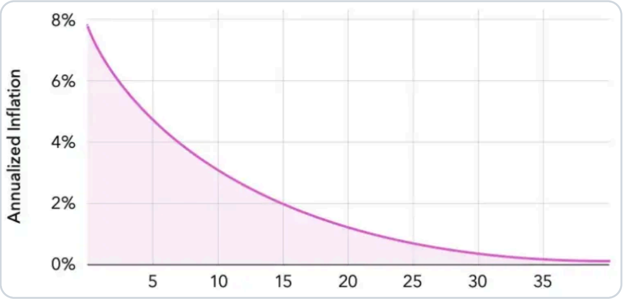
This heuristic forms a smooth exponentially decaying curve as the block_reward contributes to the current_supply which reduces the block_reward computed at the next block.

Any burns from fees or otherwise reduce current_supply and essentially become part of the budget for block rewards. The constant is chosen so that, in the absence of any burns, 99% of the coins will be emitted in about 40 years.

Block Rewards / Year



Inflation / Year



Investor Allocation

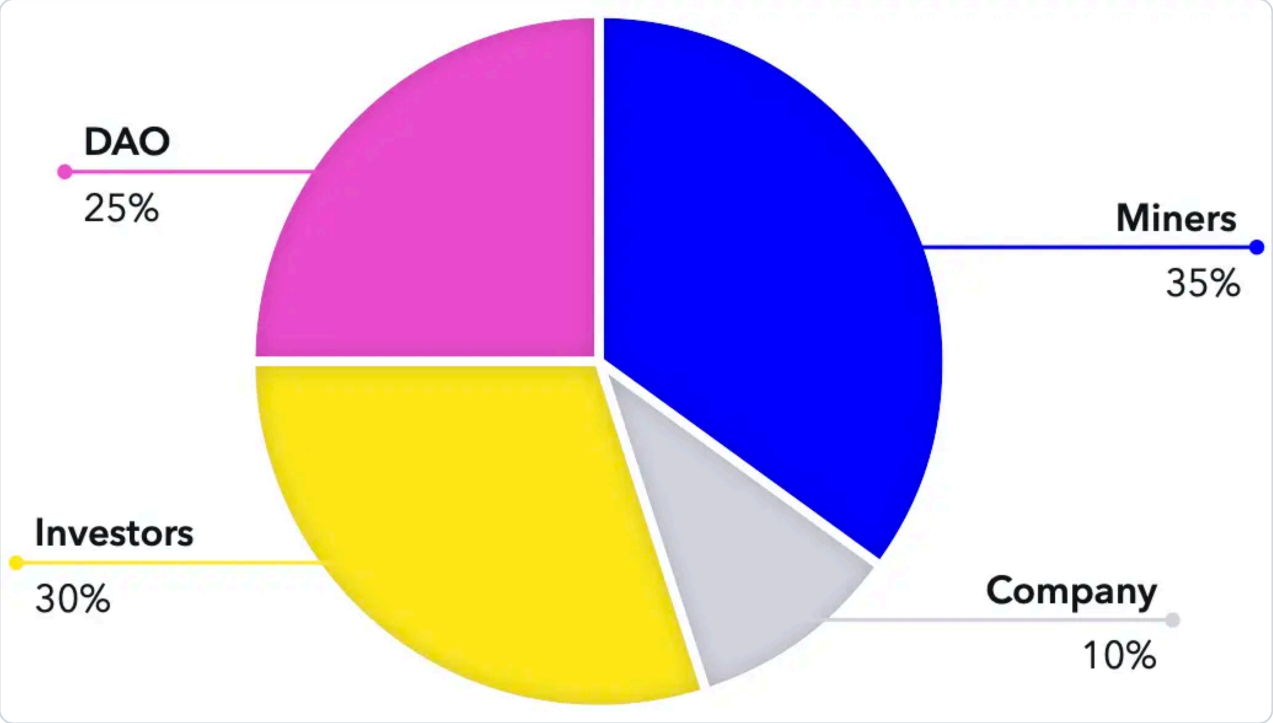
Quantus Network was built with the help of angel investors who took great risk in funding it. To avoid the supply overhangs that investor-lockups create, we are making all investors, public and private, liquid on day one. This allocation will be the only "pre-mine". All other tokens will have to be mined into existence. Depending on the success of public sales this portion will represent 20-30% of the total supply.

Company Allocation

To compensate the team for taking the risk to build new technology with no promise of success, we will divide the block rewards into two halves. First half will go to the miner. For approximately four years the second half will go to the company. This gives a de facto vesting schedule of about 10% of the total supply to the company. During this time, the miners get the same amount of newly minted coins.

After that point, the company's portion of block rewards will be redirected to a treasury governed by token holders, essentially forming a DAO.

Approximate Supply Allocation



Transaction Fees

Standard transactions will have a fee that goes to miners, providing an incentive to include transactions. Reversed transactions from high-security accounts will be charged a volume-based fee of 1% that is split, with half going to the miner and half being burned, going to the future security budget. Transactions that go thru the zk aggregation system will also be subject to a volume-based fee of 0.1%, which will be split among the miner, the proof aggregator, and a burn.

Forkless Upgrades

Quantus Network supports “forkless” upgrades through Substrate’s runtime upgrades, allowing the blockchain’s core logic (the “runtime”) to evolve without hard forks that could disrupt the network or split the community. This is achieved via on-chain governance referenda, where approved proposals trigger a runtime swap, essentially replacing the existing WASM code blob with a new one in a single block, ensuring continuity of state and operations. This upgrade path minimizes downtime and risks, empowering the community to iteratively refine the protocol.

Governance System

Quantus Network inherits its governance framework from Polkadot’s OpenGov system via Substrate. Token holders participate via conviction voting, where they agree to lock their assets for varying periods to amplify their vote’s weight. This amplification can range from 1x (no lock) to 6x (maximum lockup). This design encourages long-term alignment by tying influence to commitment.

Proposals are categorized into multiple voting tracks called “origins”. Each origin has tailored parameters like approval thresholds (e.g., supermajority for high- impact changes), minimum deposits to deter spam, preparation/enactment periods, and decision timelines to prevent gridlock. This multi-track design allows parallel processing of diverse referenda, from routine treasury spends to critical runtime upgrades.

The Technical Collective is a curated group of technical experts serving as a specialized body to propose, review, or whitelist urgent technical matters, expediting them through a dedicated track while maintaining community oversight.

Quantus adopts this system without modifications but starts with a minimalistic setup to avoid complexity in its early stages. Initially, only the Technical Collective track is active, which will be used for binding, high-privilege decisions like protocol upgrades or parameter tweaks.

Later we will introduce non-binding community vote track is for gauging sentiment on non-enforceable topics, such as feature suggestions or ecosystem polls. This system will become binding when the company turns the network over to the DAO.

This phased approach allows the network to evolve organically via future governance votes without burdening users with unnecessary complexity at the beginning.

Roadmap

Heisenberg Inception

DECEMBER 2024

Funding Secured, Substrate Chosen

Resonance Alpha

JULY 2025

Public Testnet, Dilithium Signatures, Reversible Transactions

Schrödinger Beta

OCTOBER 2025

Features Complete, Ready for Audit

Dirac Beta

NOVEMBER 2025

PoW changed to Poseidon2, Audits Addressed

Planck Beta

JANUARY 2026

High Security Accounts, Multisigs, Hardware Wallet

Bell Mainnet

Q1 2026

Mainnet Launch

Fermi Upgrade

Q2 2026

ZK Aggregation

Risks

Building Quantus Network comes with inherent risks.

- **Implementation Issues:** Flaws in software logic can cause serious failures in even the best designed systems.
- **NIST Algorithm Selection Issues:** Potential flaws or backdoors in selected post-quantum standards (e.g., ML-DSA, ML-KEM) that could emerge post- standardization. In the worst case, such flaws would allow an attacker to forge signatures by deriving a private key from the public, representing a catastrophic failure mode of the chain. If such flaws were made public, Quantus Network could be upgraded to a new algorithm, but if such flaws are exploited sparingly they may never be discovered.
- **Quantum Computing Timelines:** Quantum breakthroughs might arrive much later than anticipated, delaying the need for PQC; conversely, secretive development (e.g. by governments) could lead to sudden threats if the blockchain community fails to update swiftly.
- **Other Considerations:** General adoption barriers, regulatory uncertainties in finance/blockchain, and the inherent volatility of crypto ecosystems.

Closure

QUANTUS

We believe in the power of open protocols, proof-of-work, and sovereign ownership. The Quantus Network app, available on desktop and mobile, lets users store digital assets, mine new blocks, and participate in a fairer financial future without intermediaries.

We're committed to transparency, privacy, and empowering individuals through secure, self-custodial tools.