Quantus Network Whitepaper v0.2

Legal Disclaimer: This whitepaper is provided for informational purposes only and does not constitute an offer to sell, a solicitation of an offer to buy, or a recommendation for any security, investment, or financial product. Readers should conduct their own due diligence and consult with qualified professionals before making any decisions. Quantus Network makes no representations or warranties regarding the accuracy or completeness of the information herein.

1. 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.

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

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
- Reversible transactions to deter theft and enable recovery from mistakes
- Human-readable check-phrases for easy address checking

This targeted approach empowers users to preserve wealth confidently, turning quantum threats into opportunities. Indeed quantum computers can even mine Quantus alongside normal computers via the novel proof-of-work algorithm. Quantus is the future-proof fortress for your fortune.

Foundation

Quantus Network is built on Substrate, the blockchain SDK built by ParityTech, the team that built Ethereum and Polkadot. Substrate is highly modular, so we can easily swap components out and focus on what makes us unique without re-inventing the wheel.

2. The Quantum Threat to Blockchain

Quantum Computing Basics

Quantum computers leverage principles like superposition and entanglement to perform computations that are infeasible 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 cryptographic systems underpinning blockchain finance, as algorithms developed for quantum hardware can undermine the security assumptions of 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 a few thousand logical qubits) could derive private keys from public keys in O((log N)^3) time, where N is the modulus, 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). However, 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 catastrophic 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 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 (Dilithium)	1,312	2,560	2,420
ECDSA (256-bit)	32	32	65

As shown, ML-DSA signatures can be over 37 times larger than ECDSA equivalents, and public keys more than 40 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, particularly for finance-focused networks where high transaction volumes are critical for wealth preservation and efficient asset management.

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.

3. Quantus Network Architecture

Post-Quantum Cryptographic Primitives

Quantus Network employs NIST-standardized post-quantum cryptographic (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.

While ML-DSA-87 results in larger keys and signatures (public key: ~1,312 bytes; private key: ~2,560 bytes; signature: ~2,420 bytes), these are manageable in Quantus's early-stage network, where storage is not yet a bottleneck, and future optimizations like entangled 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).

ML-DSA-87 (NIST Level 5) was chosen for signatures due to the smaller impact of authentication on the protocol and the potential for node impersonation attacks, which could enable denial-of-service by malicious peers sending invalid messages. This attack is already mitigated by the fact that nodes are generally untrusted in the blockchain model.

ML-KEM-768 (NIST Level 3, 192-bit classical and 96-bit quantum security) balances performance for key exchange, as 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.

This hybrid approach 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 in a finance-centric blockchain.

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 "Entangled Addresses." This system leverages zero-knowledge proofs (ZKPs) generated via the Plonky2 proving system to move balance verification off-chain, allowing the chain to verify a single compact proof without processing individual signatures. Entangled Addresses enable the verification of a large number of transactions with one proof, with the public inputs (e.g., nullifiers, storage roots, 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 Poseidon for commitments via FRI (Fast Reed-Solomon Interactive Oracle Proofs, used in STARKs), instead of the quantum-vulnerable elliptic-curve pairings commonly used in SNARKs.

Additionally the authentication secrets are hidden behind Poseidon. 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
- storage roots and exit addresses are deduplicated
- 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:

- each storage root's inclusion in a recent block header
- nullifier uniqueness (to prevent double-spends)
- proof validity

The ZK circuit enforces:

- storage proof correctness
- nullifier computation accuracy
- address unspendability

Plonky2 was selected for the following reasons

- already been 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, Entangled Addresses could pack ~153k 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 entanglement 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 net-zero supply via burns.

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

Consensus Mechanism

Quantus Network uses a novel Proof-of-Work (PoW) consensus algorithm that preserves the desirable properties of Bitcoin's consensus algorithm while introducing a symbiotic relationship with quantum computing. 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. Quantus gives quantum computers an even bigger advantage by embedding an RSA factoring problem into the hash puzzle.

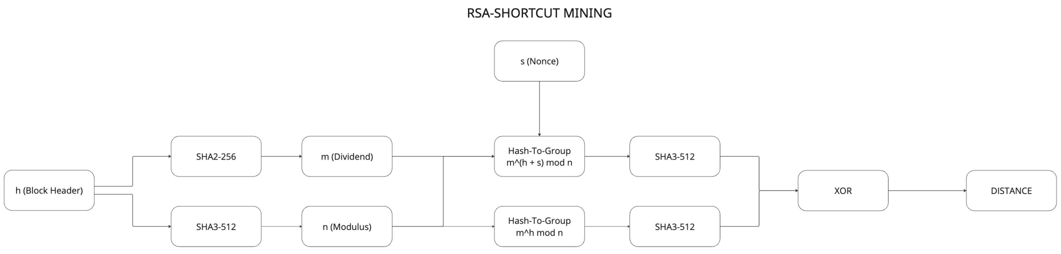
This design rewards quantum computer's participation in mining and transforms quantum threats into network security. Classical (non-quantum) miners can still brute-force "close enough" solutions by grinding nonces, while quantum miners can factor the modulus to achieve exact solutions. These exact solutions will be visible on-chain, revealing the presence of quantum miners and alerting the public to progress in quantum computing.

To compare how close this 512 bit factoring problem is to the problem of cracking a 256 elliptic curve key, consider these estimates of number of qubits and quantum gates needed for each task: (https://arxiv.org/pdf/1706.06752)

	Logical Qubits Required	Quantum Gates Required
512 RSA Problem	1026	6.41e10
256 ECDLP Problem	2330	1.27e11

Combined with the constraint of the block-time, this indicates the presence of a quantum miner, signalling that Bitcoin's keys are in danger. In this way, the Quantus Network can act as a quantum canary, paying quantum computers to both secure the network and to reveal themselves before they can crack Bitcoin keys.

Mechanism



The mechanism begins by deterministically generating a random RSA-like problem from the block header hash. Two coprime composites, m (256-bit) and n (512-bit modulus), are derived via SHA2-256 and repeated SHA3-512 applications until n is suitable (avoiding pathological cases like shared factors or primality, which could trivialize the puzzle). A function f(h, s) computes m raised to the power of (header value + nonce s) modulo n, which is then hashed with SHA3-512. The "distance" is the XOR of f(h, 0) and f(h, s), interpreted as an integer; if this distance is below the difficulty threshold t, the nonce is valid. Difficulty t adjusts dynamically based on hashrate, ensuring consistent block times. Exact solutions (distance = 0) require computing Euler's totient φ(n), which demands factoring 512-bit n, a task feasible for quantum computers via Shor's algorithm but intractable classically. This distinction allows the network to differentiate mining methods: approximate solutions indicate classical brute-force, while exact ones signal quantum involvement. Rewards are fixed per block, with the potential for governance votes to update this.

For more technical detail please see QIP-0003.

Chain Interoperability

Quantus Network can interoperate with pre-quantum blockchains thru a quantum secure bridge, built on Hyperlane. The first destination will be Solana because of its low fees and easy implementation of dilithium signature verification.

Bridges generally work by locking or burning tokens on the origin chain and unlocking or minting coins on the destination chain. Off-chain validators attest to the inclusion of the transaction on the origin chain and that attestation is sent to the destination chain by Relayers.

The contracts on either chain may have an "owner" with permissions to change critical functionality.

Each of these parties has a key that could be compromised by a quantum computer if it uses pre-quantum cryptography. Forgeries of digital signatures on a bridge can be categorized as follows:

1. Forgery of sender's signature
2. Forgery of recipient's signature
3. Forgery of contract owner's signature
4. Forgery of validator's signature
5. Forgery of relayer's signature

For the sender and recipient, these failure modes are identical to the failure mode for signature forgery on the source and destination blockchains, respectively. On the pre-quantum chain we have no control over the signatures and on the post-quantum chain this forgery is impossible, so we focus on the others.

The contract owner key would be post-quantum on the post-quantum chain, but on the pre-quantum chain it should be revoked. Forgery of a relayer's signature is generally irrelevant in the Hyperlane model. They sign a message to pay gas fee but their signatures are not involved in the security model of the bridge.

Many bridge implementations involve multiple validators in a threshold signature scheme. A sufficient number of forgeries from the various validators would enable an attacker to attest to transactions that did not get included in the chain, allowing unauthorized unlocking or minting of coins. In Hyperlane, such an attack is detectable and punishable via slashing of staked HYPER tokens, but it is still a very undesirable outcome.

This wide attack surface makes it desirable to build a quantum secure bridge. Quantus Network achieves this by building the following custom components on top of the Hyperlane infrastructure:

- PQC Validator that does attestations with ML-DSA
- PQC Interchain Security Module on both Solana and Substrate that verifies dilithium signatures from validators
- Hyperlane "Mailbox" for Substrate

For more technical details, see QIP-0012.

4. Wealth Preservation

There are a lot of ways to lose money in crypto. Many of them are avoidable. Quantus Network bakes in 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 uncancelled). 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.

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

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.

For more technical detail please see QIP-0008.

High-Security Accounts

Quantus Network's high-security accounts enhance theft deterrence by enforcing mandatory reversal periods on all outgoing transfers, allowing a designated "interceptor" 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 interceptor 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 interceptor, enabling composable hierarchies where each interceptor has superior permissions to the account it protects. This design mimicks 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 cancel recovery if they have access to their keys. This feature enables survivorship: users have an on-chain will without the need for courts or estates.

Cross-Chain Asset Wrapping

The post-quantum bridge to Solana enables widespread migration of various assets to Quantus Network, thereby quantum-securing their assets. This provides a simple way to quantum secure assets like BTC (wrapped) or USDC with the caveat that any assets held on a pre-quantum chains could still be stolen and sold, affecting the price of the assets held in post-quantum keys.

Fixing this issue completely requires the pre-quantum chains and custodians to upgrade their cryptography.

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 is 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.

5. 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.

Tokenomics

Quantus Network employs a straightforward tokenomics model featuring constant block rewards to incentivize miners to secure the chain. Miners receive transaction fees as well as an incentive to include transactions in the blocks. Reversed transactions include a volume-based fee to the miner, so that miners will prioritize these time-sensitive transactions.

The constant block reward forms a "disinflationary" model, where the inflation as a percentage trends to 0 over time. The PoW algorithm has a target block time and a self-adjusting difficulty algorithm. Changes to parameters, such as reward size or issuance schedule, can be proposed and enacted via on-chain votes. This releases the obligation to get the tokenomics "perfect" on the first try.

The initial token supply is divided into two halves, half for "insiders" (investors, team, early contributors) and half for "outsiders" (rewards, marketing, liquidity, etc.). All insider tokens are vested with a 4 year vesting schedule with no tokens vesting until after the first year. All vesting is done on-chain, transparently.

There is an on-chain "treasury" that holds funds that may be spent via an on-chain vote. This treasury collects a fixed reward for every block.

Specific amounts for each of these parameters is TBD.

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 two tracks are active:

- The Technical Collective track is for binding, high-privilege decisions like protocol upgrades or parameter tweaks.
- The non-binding community vote track is for gauging sentiment on non-enforceable topics, such as feature suggestions or ecosystem polls.

Other tracks can be introduced later as the community matures. This phased approach allows the network to evolve organically via future governance votes without burdening users with unnecessary complexity at the beginning.

6. Roadmap

The current roadmap thru 2026, subject to change:

- Heisenberg Inception - December 2024 - Funding secured, Substrate chosen
- Resonance Alpha - July 2025 - Public testnet, dilithium signatures, reversible transactions
- Schrödinger Beta - October 2025 - Feature complete, ready for audit
- Bell Mainnet - Q4 2025 / Q1 2026 - Mainnet launch
- Planck - Q2 2026 - High Security Accounts, Multisignature Accounts, Hardware Wallet Integration
- Dirac - Q3 2026 - Entangled Addresses, Bridge to Solana

7. Risks

Like anything worth doing, the Quantus Network comes with 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.