QUANTUM CHAIN

Quantum-Safe Digital Currency and Tokenization Infrastructure

TECHNICAL WHITEPAPER

JAN 2026

Quantum Chain - *Quantum–Safe Digital Currency & Tokenisation Infrastructure*
Version: Website Edition (Public)

Executive Summary

Quantum Chain is a finance–grade, permissioned blockchain infrastructure designed for sovereigns, banks, and regulated financial institutions operating in an era where classical cryptography is no longer sufficient. It delivers post–quantum security, deterministic compliance at consensus, and full EVM compatibility, enabling digital currencies, stablecoins, and tokenised financial instruments to be issued, settled, and governed with institutional assurance.
Unlike public blockchains retrofitted with post–quantum primitives, Quantum Chain is engineered from first principles for quantum resistance, regulatory determinism, and operational predictability.

1. The Problem We Solve

1.1 The Quantum Threat
Most financial blockchains rely on ECDSA, EdDSA, or RSA–based cryptography. These schemes are vulnerable to Shor–class quantum attacks. Migration paths are uncertain, fragmented, and often incompatible with live financial infrastructure.

1.2 Compliance as an Afterthought
Legacy blockchains treat compliance as an off–chain concern. This creates: - Non–deterministic enforcement - Post–facto regulatory intervention - Settlement risk at scale
Financial systems require compliance enforcement at admission, not reconciliation after execution.

1.3 Operational Instability
Probabilistic consensus, stake–weighted governance, and opaque validator incentives are misaligned with regulated financial environments that demand auditability, predictability, and accountability.

2. Design Principles

Quantum Chain is built around four non–negotiable axioms:

1. Post–Quantum by Construction
2. All ledger and network security primitives are resistant to known quantum attacks.
3. Determinism at Consensus
4. Every validator reaches the same decision given the same inputs—no randomness, no oracle ambiguity.
5. Separation of Cryptographic Roles

6. Different cryptographic primitives serve distinct functions to prevent systemic cascade failure.
7. Minimal Deviation from Proven Systems
8. Ethereum execution semantics are preserved; only cryptography and admission logic are replaced.

3. High—Level Architecture

Quantum Chain is an Ethereum—compatible, Proof—of—Authority (PoA) blockchain with a post—quantum security layer and an integrated compliance engine.
Core Components: - Validator Chain Nodes - Quantum Protocol (Cryptographic Layer) - Deterministic AI Compliance Nodes - ISO 20022 / SWIFT Ingress Gateways - Governance & Key—Management Infrastructure

4. The Quantum Protocol (Post—Quantum Security Layer)

Quantum Chain uses a dual—scheme cryptographic architecture with strict role separation.
4.1 Ledger Authenticity — CRYSTALS—Dilithium3
Used exclusively for: - Transaction signatures - Block sealing
Properties: - EUF—CMA secure against quantum adversaries - Fast verification suitable for high—throughput ledgers - Homogeneous on—ledger signature scheme (simplifies clients and audits)
4.2 Node Identity & Secure Channels — SPHINCS+
Used exclusively for: - Validator identity authentication - Inter—node handshakes - Session bootstrap
Properties: - Hash—based security (minimal assumption surface) - Long—term identity assurance - Immune to lattice—specific cryptanalytic breakthroughs
4.3 Ephemeral Key Exchange — Post—Quantum KEM
·IND—CCA secure KEM (e.g. ML—KEM / Kyber)
·Used only for ephemeral session secrets
·Provides forward secrecy when ephemeral keys are erased
4.4 Why Role Separation Matters
·A break in node identity cannot forge ledger history
·A break in ledger signatures cannot impersonate validators
·No cryptographic primitive is reused across trust domains
This prevents single—point cryptographic collapse.

5. Consensus Model — Finance—Grade Proof of Authority

Quantum Chain uses Clique Proof—of—Authority, selected deliberately.
5.1 Why PoA for Finance
·Known, audited validator set
·Deterministic block production
·Explicit governance over membership
·No probabilistic finality
5.2 Validator Guarantees
·Honest—majority assumption
·Signer—frequency limits prevent dominance
·Deterministic leader rotation
This aligns naturally with consortium banks, central banks, and regulated issuers.

6. Deterministic Compliance at Consensus

6.1 Dual–Approval Transaction Model

A transaction is accepted if and only if:

1. Cryptographically valid
2. Protocol–admissible (nonce, gas, balance)
3. Compliance–approved

All three checks are enforced by every validator.

6.2 Compliance as a Decision Function

Compliance is formalised as a deterministic function over transaction features: - Risk scoring - Rule–based constraints - Absolute prohibitions

No randomness. No external calls. No post–execution checks.

6.3 Why This Matters

·Identical compliance outcomes across all validators

·Regulatory enforcement becomes consensus truth

·Eliminates discretionary settlement risk

7. AI–Assisted, Not AI–Controlled

AI models are used only for feature evaluation and scoring.

Safeguards: - Models and parameters are pinned by governance - No online learning during consensus - Deterministic inference only

AI informs decisions; it does not arbitrate them.

8. ISO 20022 & SWIFT Integration

Quantum Chain integrates natively with financial messaging standards.

8.1 Ingress Pipeline

1. ISO 20022 / SWIFT message received
2. LLM–based semantic pre–gate (off–chain)
3. Canonical transaction mapping
4. On–chain deterministic compliance evaluation

This preserves financial semantics while ensuring blockchain determinism.

9. Tokenisation & Digital Currency Use Cases

Quantum Chain is designed to support:

·Sovereign digital currencies

·Regulated stablecoins

·Tokenised deposits

·Bonds, funds, and structured products

·Carbon credits and real–world assets

Each asset can embed: - Issuer–specific rules - Jurisdictional constraints - Lifecycle governance

10. Governance & Key Management

10.1 Validator Governance

·Explicit onboarding and removal

·Certificate–based identity

·Controlled key rotation

10.2 Key Lifecycle Discipline
·Long–term keys rotate via governance
·Ephemeral session keys erased post–handshake
·Hardware–backed key storage (HSM / TEE)

11. Security Properties (At a Glance)

·Post–quantum ledger authenticity
·Mutual entity authentication
·Forward–secure encrypted channels
·Deterministic state transitions
·No cryptographic role reuse

12. Why Quantum Chain

Quantum Chain is not a retail blockchain, a DeFi protocol, or a speculative network.
It is infrastructure: - For central banks planning beyond 2030 - For financial institutions facing quantum timelines - For issuers requiring compliance certainty
It is designed to replace—not patch—legacy settlement rails.

Contact & Engagement

Quantum Chain is deployed as a permissioned infrastructure in partnership with sovereigns, banks, and licensed issuers.
For technical evaluations, pilots, or regulatory engagements, contact:
contact@quantumcha.in

QUANTUM CHAIN

Maxwell Denega
Founder & CEO
maxwell.denega@quantumcha.in
+6582100046