QUANTUM CHAIN

QUANTUM-SAFE DIGITAL CURRENCY
AND TOKENISATION INFRASTRUCTURE

JANUARY 2026

TECHNICAL WHITEPAPER

Post-quantum security, deterministic compliance and full EVM compatibility for sovereigns, banks and regulated financial institutions.

EDITION
Website Edition (Public)

PUBLISHED
January 2026

CLASSIFICATION
Public

QUANTUMCHA.IN/REQUEST-PILOT

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 five non-negotiable axioms:

AXIOM 01

Post-Quantum by Construction

All ledger and network security primitives are resistant to known quantum attacks.

AXIOM 02

Determinism at Consensus

Every validator reaches the same decision given the same inputs — no randomness, no oracle ambiguity.

AXIOM 03

Separation of Cryptographic Roles

Different cryptographic primitives serve distinct functions to prevent systemic cascade failure.

AXIOM 04

Minimal Deviation from Proven Systems

Ethereum execution semantics are preserved; only cryptography and admission logic are replaced.

AXIOM 05

Public-Permissioned by Design

Permissioned control and public reach are not mutually exclusive. Institutions govern their own network perimeter while retaining access to public distribution for the assets they issue.

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	Quantum Private Network (QPN) Subnets

4 Network Topology — Public-Permissioned by Design

Quantum Chain is public-permissioned. Validation, admission and governance remain permissioned and accountable, but the network is not confined to a single closed perimeter: institutions can operate privately and distribute publicly on the same protocol.

4.1 Quantum Private Networks

Regulated institutions can launch **Quantum Private Networks** — sovereign or institution-scoped networks that inherit the full Quantum Chain stack.

- Post-quantum cryptography and deterministic compliance enabled by default
- Institution-controlled validator set, membership and governance
- Transaction visibility restricted to authorised participants and supervisors
- Suited to tokenised deposits, intra-group settlement and any workload where operational privacy is a supervisory requirement

4.2 Public Distribution Where It Is Wanted

The same issuer can reach the public permissioned network without re-platforming.

- Assets issued inside a private network can be distributed, held and transferred on the public network under issuer-defined rules
- Jurisdictional, eligibility and lifecycle constraints travel with the asset across both domains
- Compliance is evaluated deterministically in either environment — an asset does not lose its rulebook when it crosses networks

4.3 Why This Matters

- Banks and central banks retain operational privacy without fragmenting into isolated, non-interoperable silos
- Distribution reach becomes a per-asset decision rather than a per-platform commitment
- One protocol, one cryptographic standard and one compliance model across private and public deployment

DESIGN INTENT

Privacy where it is required. Reach where it is valuable.

5 The Quantum Protocol — Post-Quantum Security Layer

Quantum Chain uses a dual-scheme cryptographic architecture with strict role separation.

5.1 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)

5.2 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

5.3 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

5.4 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

NET EFFECT

This prevents **single-point cryptographic collapse**.

5.5 Cryptographic Agility

Quantum Chain is built crypto-agile. Cryptographic primitives are treated as versioned, governed parameters rather than hard-coded assumptions.

- Algorithm identifiers are carried explicitly in transaction, block and handshake formats
- Signature, KEM and hash schemes can be introduced, deprecated or rotated through governance without altering execution semantics
- Dual-scheme transition windows allow outgoing and incoming primitives to be accepted concurrently during migration
- Role separation means each primitive can be replaced independently, containing the blast radius of any future cryptanalytic advance

WHY IT MATTERS

The post-quantum standards landscape will continue to evolve. Crypto-agility ensures Quantum Chain can adopt future standards without re-platforming, forking history, or interrupting live settlement.

6 Consensus Model — Finance-Grade Proof of Authority

Quantum Chain uses Clique Proof-of-Authority, selected deliberately.

6.1 Why PoA for Finance

- Known, audited validator set
- Deterministic block production
- Explicit governance over membership
- No probabilistic finality

6.2 Validator Guarantees

- Honest-majority assumption
- Signer-frequency limits prevent dominance
- Deterministic leader rotation

This aligns naturally with consortium banks, central banks and regulated issuers.

7 Deterministic Compliance at Consensus

7.1 Dual-Approval Transaction Model

A transaction is accepted if and only if it is:

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

All three checks are enforced by every validator.

7.2 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.

7.3 Why This Matters

- Identical compliance outcomes across all validators
- Regulatory enforcement becomes consensus truth
- Eliminates discretionary settlement risk

8 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

> **PRINCIPLE**
>
> AI **informs** decisions; it does not **arbitrate** them.

9 ISO 20022 & SWIFT Integration

Quantum Chain integrates natively with financial messaging standards.

9.1 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.

10 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

11 Governance & Key Management

11.1 Validator Governance

- Explicit onboarding and removal
- Certificate-based identity
- Controlled key rotation

11.2 Key Lifecycle Discipline

- Long-term keys rotate via governance
- Ephemeral session keys erased post-handshake
- Hardware-backed key storage (HSM / TEE)

12 Security Properties at a Glance

Post-quantum ledger authenticity	Mutual entity authentication
Forward-secure encrypted channels	Deterministic state transitions
No cryptographic role reuse	Crypto-agile primitive rotation under governance

13 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

POSITIONING

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

QUANTUMCHA.IN/REQUEST-PILOT