QUANTUM

The First EVM-Compatible Layer 1
Engineered for the Post-Quantum Era

PQ-Secure from Genesis | Sub-Second Finality | Full EVM Compatibility

Built by **MultiVM Labs**

THE PROBLEM

The $3 Trillion Security Debt

Every major blockchain relies on ECDSA — cryptography that quantum computers will break via Shor's algorithm.

$3T+
digital assets secured by breakable cryptography

6.8M
BTC with exposed public keys — directly vulnerable

2028–35
expert estimates for "Q-Day" — when ECDSA breaks

! "Harvest Now, Decrypt Later" attacks are happening **today**. Stolen data will be decrypted when quantum arrives.

THE TIMELINE

Q-Day Is Not Theoretical

2024 ✓ **NIST finalizes PQC standards**

FIPS 203 / 204 / 205 published. Algorithm question settled.

2024 ✓ **Google Willow: 105 qubits**

First chip with below-threshold error correction.

2026 **U.S. federal PQC mandate**

Federal systems must be PQC-capable. Compliance clock starts.

2028–35 **Q-Day: ECDSA breaks**

Shor's algorithm on fault-tolerant quantum computers.

2030 **NIST deprecates RSA / ECDSA**

Legacy cryptography officially retired.

THE GAP

Why Existing Chains Can't Just "Upgrade"

DIMENSION	LEGACY CHAINS	QUANTUM
Migration Path	✗ Contentious hard forks	✓ PQ-native from genesis
State Migration	✗ Billions of accounts to migrate	✓ No legacy accounts
Signature Sizes	✗ 10–100× larger — protocol can't handle	✓ Protocol designed for PQ payloads
Consensus	✗ Not tuned for large sigs	✓ Simplex optimized for PQ overhead
Backward Compat	✗ Breaks wallets, dApps, tooling	✓ Full EVM compat, no debt
Coordination	✗ Validators, wallets, dApps must align	✓ Single coherent design
Crypto Agility	✗ Locked to one scheme	✓ Hedging modes + algorithm upgrades
Time to Secure	✗ Years of migration risk	✓ Secure on day one

THE SOLUTION

Quantum: Post-Quantum Secure by Default

An EVM-compatible L1 designed for a world where PQ authorization is non-optional.

PQ-by-Default

NIST-standardized Falcon & ML-DSA signatures from genesis. No ECDSA. Zero legacy debt.

Sub-Second Finality

Engineered around the PQ Scaling Cliff — larger keys, no performance sacrifice.

EVM Compatible

Built on Reth. Full compatibility with Solidity, Foundry, Hardhat.

Crypto-Agile

Hedging modes from Normal to Emergency. Built to survive algorithm surprises.

ARCHITECTURE

Engineered for the PQ-Scaling Reality

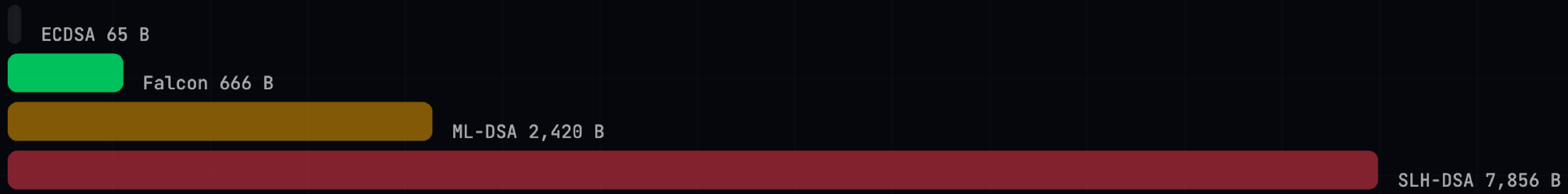
1	**Execution**	Reth-based EVM — full Ethereum execution ergonomics	CORE
2	**Consensus**	Commonware Simplex — 2 hops notarization, 3 hops finalization	PROTOCOL
3	**Authorization**	PQ tx type + Falcon / ML-DSA verifier precompiles	SECURITY
4	**Entanglement Bridge**	LayerZero v2 + DVN stack + PQ boundary gate	INTEROP
5	**PQ Wallet Layer**	MetaMask Snap + Local Signer + PQ Smart Wallets on other chains	CLIENT
6	**QCN**	Quantum Circuit Network — decentralized QPU marketplace	APPLICATION

CRYPTOGRAPHY

NIST-Standardized Post-Quantum Signatures

SCHEME	STANDARD	SIG SIZE	ROLE
Falcon-512	FIPS 206 (planned)	≤ 666 B	Primary — compact, high throughput
ML-DSA-44	FIPS 204	2,420 B	Conservative fallback — battle-tested
SLH-DSA 128s	FIPS 205	7,856 B	Break-glass hedge — hash-based safety

Signature size comparison (ECDSA = 65 B)



This is why you can't just bolt on PQ crypto — the protocol must be designed for it.

THE CHALLENGE

The PQ Scaling Cliff

PQ signatures are CPU-manageable, but they are *large* — and that cascades everywhere.

User Layer

`10-100× larger payloads`

Fewer TXs per block at same byte budget. Increased propagation latency and orphan risk.

Consensus Layer

`~44.6 KB per quorum proof`

Quorum proofs: (2f+1) × sig_size. 200 validators → ~88.6 KB. Bandwidth dominates.

Our Approach

- ✓ Protocol designed for PQ constraints from day 1
- ✓ Ringtail threshold certificates → 99% compression
- ✓ Simplex consensus with minimal critical path
- ✓ Bandwidth & storage budgets PQ-aware

CRYPTOGRAPHIC AGILITY

Built to Survive Algorithm Surprises

If lattice-based crypto is ever broken, we have a contingency plan — not a panic.

Normal

Lattice-only signatures (Falcon / ML-DSA). Maximum performance.

Checkpoint-Hedged

Hash-based signatures (SLH-DSA) at epoch boundaries. Safety with minimal overhead.

Emergency

Dual-sign every message: lattice + hash-based. Maximum safety under active attack.

Vault accounts (2-of-2): Users can opt into dual-key accounts — one lattice key + one hash-based key. Both required to spend.

GO-TO-MARKET

The "Trojan Horse" Strategy

We don't need the world to migrate to our L1 to start acquiring users today.

1

MetaMask Snap

Install PQ signing in existing wallet

→

2

PQ Smart Wallet

Deploy on any EVM chain

→

3

Deposit & Protect

Wallet only accepts PQ sigs

→

4

Quantum-Safe

Assets safe even if ECDSA is cracked

→ Users start with PQ wallets on other chains, then naturally migrate to Quantum L1 for full PQ security.

CROSS-CHAIN

Native Post Quantum Bridge — Entanglement

Most bridges introduce risk. Ours enforces a hard security boundary.

Invariant: Nothing materializes on Quantum without post-quantum authorization.

A Marketplace for Real Quantum Compute

Quantum isn't just a ledger. It's the settlement layer for the quantum computing era.

PROTOCOL FLOW

Submit Job
Client posts circuit + stake

Accept & Bond
QPU provider bonds collateral

Commit
Provider commits result hash

Reveal
Result revealed on-chain

Finalize
Settlement & payout

WHO USES QCN

Pharma & Life Sciences
Drug discovery simulations

Financial Services
Portfolio & risk optimization

Algorithm Research
Quantum algorithm benchmarking

Hardware Providers
Monetize idle QPU capacity

USE CASES

Who Needs Quantum Today?

Anyone holding assets that must be secure 10+ years from now.

Institutional Custody

Treasuries & vaults immune to "harvest now, decrypt later"

Real World Assets

Tokenized bonds & real estate with multi-decade lifecycles

Government & Defense

Infrastructure requiring FIPS-compliant PQC standards

Long-Horizon Governance

Voting that remains valid under future quantum threats

High-Value Vaults

Break-glass safety with dual-sign policies

Compute Settlement

QPU job results anchored under PQ authorization via QCN

MARKET OPPORTUNITY

The Sanctuary for Long-Lived Value

MARKET SIZE

$2.8B 46% CAGR
PQC market by 2030

$3T+
crypto assets at risk from quantum

$16T+
projected tokenized RWA market by 2030

GROWTH DRIVERS

Regulatory Push
2026 U.S. federal PQC mandate. NIST deprecating RSA/ECDSA by 2030.

Institutional Demand
Custody providers and exchanges need quantum-safe infrastructure.

RWA Explosion
Multi-decade assets on-chain require multi-decade security guarantees.

COMPETITIVE LANDSCAPE

Why Quantum Wins

	QUANTUM	ETHEREUM	QRL	OTHER L1S
PQ from Genesis	✓	—	✓	—
EVM Compatible	✓	✓	—	Varies
Sub-Second Finality	✓	—	—	Varies
NIST Standards (FIPS)	✓	—	XMSS only	—
Cross-Chain PQ Wallets	✓	—	—	—
Quantum Compute Marketplace	✓	—	—	—
Crypto-Agile Hedging	✓	—	—	—

TOKEN

$QBIT — Native Protocol Token

Staking

Secure the network through PQ-authenticated validator staking

Gas Fees

Pay for execution on the Quantum L1

QCN Payments

Settlement currency for quantum compute jobs

Governance

Protocol governance with PQ-secured voting

Quantum-Wrapped Assets

qBTC qETH qSOL qUSDT **QBIT**

ROADMAP

Path to Mainnet

01 Devnets — Now

- PQ consensus baseline (Simplex + Falcon)
- PQ userland authorization + precompiles
- Checkpoint hedging & emergency mode
- Key registry (AuthDescriptor)

02 Testnet

- PQ Wallet Layer (Snap + Smart Wallets)
- Entanglement bridge integration
- Developer tooling (Foundry / Hardhat)
- Multiple independent audits

03 Mainnet

- Launch with Falcon / ML-DSA
- $QBIT Token Generation Event
- Bug bounty program

04 Post-Launch

- P2P transport PQ-KEM evaluation
- Quantum Circuit Network scaling
- Expanded wallet integrations

TRACTION

Momentum & Validation

MILESTONES

- ✓ Testnet live with quantum tokenization
- ✓ NIST FIPS 203/204/205 aligned
- ○ Ringtail threshold sig research
- ✓ EVM dApp environment with PQ tools
- ✓ Crypto-agile hedging framework
- ○ PQ Wallet Layer (MetaMask Snap)

KEY PROOF POINTS

Testnet Live
`5 wrapped assets`
qSOL, qUSDT, qETH, qBTC, QBIT

NIST Standards
`3 FIPS standards`
FIPS 203, 204, 205 — U.S. government PQC

Novel Research
`99% compression`
Ringtail threshold certificates exploration

Dev-Ready
`Full EVM`
Foundry, Hardhat, Solidity compatible

> *"The question isn't whether blockchain cryptography will break — it's whether you'll be ready when it does."*

THE TEAM

Built by MultiVM Labs

$700M+	8+	3
TOTAL VALUE SECURED	TIER-1 COMPANY ALUMNI	STARTUPS FOUNDED

>$100M
PORTFOLIO OPERATED

Ivan Miskovic
CEO & Co-Founder

Delivery Hero · Deliveroo · TGE Cap.

$600M+
TVL SECURED

Timur Guvenkaya
CTO & Co-Founder

Halborn · NEAR · Aurora

11+yr
BD & PARTNERSHIPS

Dino Ivankovic
COO & Co-Founder

Umbrella · A1 Telekom · Tele2

ENGINEERING

Ross Nkama	Martin Joly	Ryan Steubs	Erhan Acet	Ruben Marcus
Google · Meta AI	Mistral AI	Halborn	NEXT AI	Nike · Samsung

QUANTUM

EXPERTISE & BACKERS

Deep Technical DNA

Cryptography

3 NIST Standards

- FIPS 203/204/205
- Falcon
- ML-DSA
- SLH-DSA
- Ringtail
- Crypto-agile

Consensus

Sub-Second Finality

- Commonware Simplex
- Fault-tolerant
- PQ-aware bandwidth
- 2-hop notarization

Execution

Full EVM Compat

- Reth-based
- Solidity
- Foundry
- Hardhat
- PQ precompiles

BACKED BY

- Inception
- IOBC Capital
- Laser Digital
- Lattice
- Lemniscap
- Lyrik Ventures
- Maelstrom
- Public Works

QUANTUM

Secure the Future.

We are raising to finalize Mainnet engineering, audit our novel PQ-primitives, and capture the "Day 0" market for quantum-safe custody.

quantum.systems · multivmlabs.com · info@multivmlabs.com

Built by **MultiVM Labs**