Blockchains and Distributed Ledgers Quantum Transition Roadmaps

*As of **December 2025**, the "Quantum Day" (Q-Day) readiness of blockchain and Distributed Ledger Technology (DLT) has transitioned from theoretical research to active implementation. While a cryptographically relevant quantum computer (CRQC) is a few years away, the "Harvest Now, Decrypt Later" threat has forced major networks to begin their migrations this year.*

Check the comparison readiness roadmap chart based on the latest 2025 industry updates.

DLT Quantum Readiness Comparison (Dec 2025)

Blockchain / DLT	Readiness Level	Primary Migration Strategy	Key 2025 Milestone
Ethereum	**Advanced**	**"Quantum Emergency" Fork** + Account Abstraction (ERC-4337) to force PQC wallet migration.	Vitalik Buterin published a 4-year "Quantum Emergency" hard-fork plan (Dec 2025).
Solana	**Frontrunner**	**Direct PQC Integration**; deploying ML-DSA (Dilithium) signatures natively.	First major L1 to deploy post-quantum digital signatures on **Testnet** (Dec 16, 2025).
Bitcoin	**Conservative**	**Voluntary Soft Fork**; new address types (like Taproot) using quantum-safe hash-based signatures.	Community consensus growing for a PQC soft fork by 2026/2027 to protect stagnant coins.
Cardano	**Moderate**	**NIST/NATO Standard Alignment**; modular "Midnight" sidechain for PQC experimentation.	Integration of **Dilithium-5** signatures into its broader security infrastructure audits.
Enterprise (Fabric/Corda)	**High**	**Crypto-Agility**; modular BCCSP allows swapping to NIST-approved	BIS (Bank for International Settlements) released a 2025

		(FIPS 203/204) providers.	Roadmap for PQC in financial systems.

Blockchain Quantum-Day Readiness Roadmap (2025–2030)

The transition is following a three-phase progression. Public chains focus on "Account Abstraction" (self-migration), while enterprise chains focus on "Crypto-Agility" (modular swaps).

Phase 1: Inventory & Protocol Prototyping (2025 - 2026)

- **Cryptographic Audit:** Networks are identifying "vulnerable TVL" (Total Value Locked) residing in old Elliptic Curve (ECDSA) addresses.
- **Testnet Deployments:** As seen with Solana and Ethereum L2s, PQC signatures (ML-DSA) are being tested for latency and gas-cost impacts.
- **Address Rotation:** Wallets (Ledger, Trezor) are introducing "Quantum-Safe" address generation for users.

Phase 2: Hybrid Adoption (2026 - 2028)

- **Dual-Signatures:** Transactions will require both a classical signature (for backward compatibility) and a PQC signature (for future safety).
- **Account Abstraction Mandates:** Ethereum and Layer 2s will likely deprecate "Legacy" Externally Owned Accounts (EOAs), forcing users to move funds to smart contract wallets that support PQC.
- **Hardware Acceleration:** Development of specialized ASICs to handle the 10x–50x larger signature sizes of lattice-based cryptography.

Phase 3: The Native Post-Quantum Era (2029+)

- **Classical Deprecation:** Major networks disable legacy signature schemes entirely. Any funds not migrated are "frozen" behind an emergency recovery protocol.
- **Zero-Knowledge PQC:** Adoption of quantum-resistant ZK-Proofs to maintain privacy without vulnerability to Shor’s algorithm.
- **Network Settlement:** High-value settlement (CBDCs, Institutional Assets) will move exclusively to "Quantum-Hardened" DLTs.

Technical Trade-offs: The "Trilemma" of PQC

When blockchains choose an algorithm, they must balance three factors:

Algorithm	Size (Key/Sig)	Verification Speed	Storage Impact
ML-DSA (Dilithium)	Moderate (~2.5KB)	**Extremely Fast**	Moderate (increases chain bloat)
SLH-DSA (SPHINCS+)	Large (~30KB)	Slow	**High** (not ideal for high-throughput L1s)
FALCON	**Small (~0.6KB)**	Fast	Low (best for space-constrained chains)

> **Strategic Note: The biggest risk in 2025 is "Harvest Now, Decrypt Later." Adversaries are recording encrypted on-chain data today. If your data (or private transaction details) must remain secret for 10+ years, you must use PQC wrapping now, even before the first CRQC is built.**

The following sources represent the primary technical proposals, institutional roadmaps, and network updates that inform the 2025 Quantum Readiness comparison.

1. Core Protocol Roadmaps & Proposals

- **Ethereum (Vitalik Buterin's Emergency Plan):**
  - ***Source:*** **Buterin, V. (2025). "How to Save Ethereum from a Quantum Emergency." Updated proposal discussed at Devconnect Buenos Aires (Nov 2025) and various Ethereum Magicians threads regarding EIP-7702 and account abstraction.**
  - ***Focus:*** **A "simple recovery fork" to transition funds to STARK-based or lattice-based smart contract wallets if ECDSA is compromised.**
- **Solana (Project Eleven Collaboration):**
  - ***Source:*** **Solana Foundation Press Release (Dec 16, 2025). "Project Eleven to Advance Post-Quantum Security for the Solana Network."**
  - ***Focus:*** **Implementation of ML-DSA (Dilithium) signatures on the Solana Testnet and the full "Quantum Threat Assessment" report.**

- Aptos (AIP-137):
    - *Source:* Aptos Improvement Proposal (AIP) 137 (Dec 2025). "Optional Post-Quantum Account Signatures."
    - *Focus:* Integrating SLH-DSA (FIPS 205) as an opt-in security layer for users.

---

2. Institutional & Regulatory Frameworks

- Bank for International Settlements (BIS):
    - *Source:* BIS Papers No. 158 (July/Nov 2025). *"Quantum-readiness for the financial system: a roadmap."*
    - *Focus:* A three-phase migration framework (Inventory, Planning, Execution) specifically for global financial market infrastructures (FMIs) and CBDCs.
- U.S. Securities and Exchange Commission (SEC):
    - *Source:* Daniel Bruno Corvelo Costa (Sept 3, 2025). *"Post-Quantum Financial Infrastructure Framework (PQFIF)."*
    - *Focus:* A strategic framework submitted to the U.S. Crypto Assets Task Force to neutralize "Harvest Now, Decrypt Later" risks in digital asset custody.
- NIST Cryptographic Standards:
    - *Source:* NIST FIPS 203, 204, and 205 (Finalized 2024, implementation guidance updated 2025).
    - *Focus:* The formal standardization of ML-KEM (Kyber), ML-DSA (Dilithium), and SLH-DSA (SPHINCS+) which serve as the "blueprints" for all blockchain PQC upgrades.

---

3. Expert Analysis & Industry Reports

- Metaculus & Prediction Markets (2025): * Frequently cited by Vitalik Buterin and others, placing a ~20% probability on a cryptographically relevant quantum computer (CRQC) by 2030.
- GFTN (Global Finance & Technology Network):
    - *Source:* "Quantum: Shaping The Next Decade of Financial Technologies" (Oct 2025).
    - *Focus:* Comparative analysis of how different L1/L2 networks are balancing the trade-off between signature size and network throughput.

Summary of Algorithms Used in Roadmaps

Source Authority	Recommended Algorithm	Primary Use Case
NIST (FIPS 204)	ML-DSA (Dilithium)	General digital signatures (transactions)
Solana / Aptos	ML-DSA / SLH-DSA	Testnet signatures and opt-in user security
Vitalik Buterin	STARKs / Winternitz	Quantum-safe account recovery and ZK-rollups
BIS / SEC	Hybrid (Lattice + Classical)	High-value settlement and data at rest