

Post-Quantum Migration Is More Than Replacing Signatures

A short note on crypto-agility in blockchain systems

Valentina Rivas | [Valens Research](#) | BGIN Block 15 | October 2026

Post-quantum migration in blockchain systems is sometimes framed as replacing a quantum-vulnerable signature scheme with a standardized post-quantum alternative such as ML-DSA or SLH-DSA. That replacement is necessary where vulnerable public-key cryptography is used, but it is only one part of the migration problem. Cryptographic primitives sit inside transaction formats, key and address models, wallet software, validation rules, hardware, infrastructure, and interoperability assumptions. Migration therefore has to preserve the security and operability of the surrounding system while its cryptographic dependencies change.

1. The primitive is only one dependency

Changing a signature primitive can affect much more than signature verification. Public-key and signature sizes may change; wallets may need new key-generation, recovery, and rotation flows; transaction encodings and validation logic may need modification; existing funds or accounts may remain tied to legacy keys; and nodes, hardware devices, SDKs, exchanges, custodians, and other infrastructure may not upgrade simultaneously.

For that reason, a correct implementation of a NIST-standardized post-quantum signature scheme does not by itself demonstrate that a blockchain system is ready to migrate.

2. Migration is a system problem

A migration design should make the dependencies around the cryptographic primitive explicit. At minimum, it is useful to examine:

- **Key and address lifecycle:** How new keys are introduced, rotated, recovered, and represented.
- **Transaction and validation rules:** What changes in serialization, verification, fees, or resource use.
- **Legacy state:** How existing accounts, dormant funds, and previously valid signatures remain usable or migrate.
- **Ecosystem compatibility:** What wallets, hardware, libraries, custodians, exchanges, and nodes must change.
- **Deployment path:** Whether classical and post-quantum mechanisms can coexist during a staged transition.

3. Crypto-agility should survive the migration

A migration should avoid simply hard-coding a new primitive and recreating the same transition problem for the future. At the system level, crypto-agility means being able to change cryptographic mechanisms with bounded disruption to dependent components, while maintaining clear rules for compatibility, validation, and deployment.

Post-quantum migration is therefore also an opportunity to ask whether cryptographic dependencies are sufficiently modular, versioned, and governable to support future changes.

4. Five practical questions

The following questions are intended as a compact discussion lens, not a replacement for a formal migration rubric or benchmark:

#	Question	What it reveals
1	What cryptographic assumption is changing?	Identify the primitive, keys, and security properties affected.
2	What else depends on it?	Map protocol, wallet, infrastructure, and operational dependencies.
3	Can old and new mechanisms coexist?	Determine whether a staged or hybrid transition can preserve existing state and validity rules.
4	Who has to upgrade?	Identify required changes across users, wallets, nodes, hardware, services, and other ecosystem participants.
5	Does the design improve future crypto-agility?	Ask whether the next cryptographic transition becomes easier, rather than merely replacing one fixed primitive with another.

Takeaway

A post-quantum blockchain is not defined only by the signature scheme it adopts. Migration readiness also depends on whether the surrounding system can introduce, operate, and later replace cryptography without unsafe or impractical disruption.

Relation to BGIN's PQC Migration work

BGIN's current PQC Migration work focuses on deployment, staged rollout, crypto-agility patterns, migration playbooks, and neutral evaluation of PQ readiness. This note offers a small practitioner-oriented lens for that work: primitive-level adoption should be evaluated together with the dependencies and transition mechanisms that make migration operationally viable.

Selected references

- NIST, FIPS 204, Module-Lattice-Based Digital Signature Standard (ML-DSA), August 2024.
- NIST, FIPS 205, Stateless Hash-Based Digital Signature Standard (SLH-DSA), August 2024.
- BGIN, PQC Migration project hub, 2026.
- BGIN, Post-Quantum Cryptography Migration on DLTs: Deployment, Agility & Governance, GDC 2026 meeting report, September 2026.