Post-Quantum Migration Strategy for Production Blockchain Networks

Zach Kelling

Lux Industries

2024

Abstract

We present a three-phase migration strategy for transitioning production blockchain networks from classical to post-quantum cryptography. The migration must be gradual—a hard cutover risks breaking every wallet, validator, and application simultaneously. Phase 1 deploys hybrid signatures (classical ECDSA/BLS + post-quantum ML-DSA) where both must verify. Phase 2 makes the post-quantum signature primary with the classical signature as fallback. Phase 3 deprecates classical signatures entirely. We formalize the concept of *crypto agility*: the ability to add, replace, or remove cryptographic algorithms without hard fork. We specify the key management requirements during transition, where validators maintain four key types simultaneously (EC secp256k1, BLS12-381, ML-DSA-65, Pulsar Module-LWE). We define backward compatibility rules ensuring old clients can verify classical signatures while new clients verify both. We provide concrete upgrade paths for existing validators and analyze the NIST standardization timeline (FIPS 203/204/205 published August 2024) as the basis for each phase trigger. The Lux network is currently in Phase 1 with triple-proof consensus providing hybrid classical/PQ security since genesis.

1 Introduction

The threat from cryptographically relevant quantum computers (CRQCs) is not binary. There is no single day when "quantum breaks crypto." The timeline is gradual:

1. **2024**: NIST publishes FIPS 203 (ML-KEM), 204 (ML-DSA), 205 (SLH-DSA).
2. **2025–2028**: Government mandates for PQ migration (NSA CNSA 2.0, NIST IR 8547).
3. **2030–2035**: Estimated window for first CRQCs with >4,000 logical qubits.
4. **2035+**: Potential for CRQCs capable of breaking 256-bit elliptic curves.

A blockchain network that waits until CRQCs exist is already compromised: historical transactions signed with ECDSA can be retroactively forged. The "harvest now, decrypt later" attack means adversaries are already recording blockchain data for future quantum decryption.

Migration must begin now, proceed gradually, and never require a flag day where every participant upgrades simultaneously.

2 Crypto Agility

Definition 2.1 (Crypto Agility)**.** *A system is* crypto-agile *if it can add, replace, or deprecate cryptographic algorithms without requiring a coordinated, simultaneous upgrade of all participants.*

Crypto agility in a blockchain context requires:

1. **Algorithm negotiation**: Signatures, key exchanges, and hashes are identified by algorithm IDs, not hardcoded.
2. **Multi-algorithm support**: The verification path can check multiple signature types per transaction/block.
3. **Graceful deprecation**: Old algorithms can be disabled via governance without hard fork.
4. **Key rotation**: Validators can rotate to new key types without losing their stake or identity.

2.1 Algorithm Registry

The Lux P-Chain maintains a registry of supported algorithms:

ID	Algorithm	Purpose	Status
`0x01`	secp256k1 (ECDSA)	EVM transactions, addresses	Active
`0x02`	BLS12-381	Consensus aggregation	Active
`0x03`	ML-DSA-65 (FIPS 204)	PQ identity signatures	Active
`0x04`	ML-DSA-87 (FIPS 204)	PQ high-security signatures	Reserved
`0x05`	SLH-DSA-128s (FIPS 205)	Hash-based fallback	Reserved
`0x06`	Pulsar (Module-LWE)	PQ anonymous threshold	Active
`0x07`	ML-KEM-768 (FIPS 203)	PQ key encapsulation	Active

New algorithms are added by P-Chain governance proposal. Deprecation follows the same process with a mandatory grace period.

3 Phase 1: Hybrid Deployment

Status: Active (since Lux genesis).

In Phase 1, both classical and post-quantum signatures coexist. The security guarantee is: the system is secure if *either* the classical or the post-quantum scheme is unbroken.

3.1 Dual Signature Model

Every validator registers four keys on the P-Chain:

Key Type	Algorithm	Size	Purpose
EC key	secp256k1	33 B (compressed)	EVM address derivation
BLS key	BLS12-381	48 B	Per-block consensus aggregation
ML-DSA key	ML-DSA-65	1,952 B	Per-epoch PQ identity
Pulsar key	Module-LWE	2,048 B	Per-epoch PQ anonymous threshold

3.2 Per-Block Verification (Classical)

Each block contains a BLS aggregate signature. Verification:

$$\text{BLS.Verify}(\text{aggPK}, \text{blockHash}, \sigma_{BLS}) \stackrel{?}{=} \text{true}$$

This provides sub-millisecond consensus for real-time block production.

3.3 Per-Epoch Verification (PQ)

Each epoch (1,000 blocks = 1 second) contains a STARK proof compressing N ML-DSA signatures and a Pulsar threshold signature:

$$\text{STARK.Verify}(\pi, \text{epochDigest}) \stackrel{?}{=} \text{true}$$

This provides post-quantum finality without per-block overhead.

3.4 Hybrid Security Property

Theorem 3.1 (Hybrid Security)**.** *If either (a) the BLS discrete logarithm problem is hard, or (b) the Module-LWE problem (ML-DSA) and Module-LWE problem (Pulsar) are hard, then the consensus mechanism is secure.*

Proof. The BLS aggregate provides classical security per-block. The STARK-compressed ML-DSA + Pulsar provides post-quantum security per-epoch. An adversary must break both to forge a finalized epoch. Since the two are based on independent mathematical problems (discrete log vs. lattice), compromising one does not help with the other. □

4 Phase 2: PQ Primary with Classical Fallback

Status: Planned.

Phase 2 inverts the priority: the post-quantum signature becomes the primary verification path, and the classical signature serves as a fallback for backward compatibility.

4.1 Trigger Conditions

Phase 2 activates when:

1. >90% of validators have registered ML-DSA keys (already 100% on Lux).
2. NIST finalizes additional PQ algorithms beyond FIPS 203/204/205.
3. Government mandates require PQ-primary deployment (NSA CNSA 2.0 timeline: 2030).
4. OR: credible evidence of CRQC development accelerating beyond current projections.

4.2 Changes from Phase 1

Component	Phase 1	Phase 2
Per-block consensus	BLS (primary)	ML-DSA individual sigs (primary)
Per-block fallback	None	BLS (fallback, for old clients)
Per-epoch proof	STARK(ML-DSA + Pulsar)	STARK(ML-DSA + Pulsar)
Block header size	144 B	∼3,500 B (ML-DSA sig included)
Verification order	BLS first, then epoch PQ	ML-DSA first, BLS optional

The block header size increase (144 B → ∼3,500 B) is the primary cost of Phase 2. This is mitigated by STARK aggregation at the epoch level.

4.3 Backward Compatibility

Old clients (Phase 1 software) continue to function by verifying the BLS fallback signature. They do not verify the ML-DSA primary signature but are not required to—the BLS signature remains valid.

Property 4.1 (Backward Compatibility)**.** *A Phase 1 client can verify all blocks produced by a Phase 2 network by checking only the BLS aggregate signature. It cannot verify post-quantum finality but can verify classical finality.*

5 Phase 3: Pure Post-Quantum

Status: Future.

Phase 3 removes classical cryptography from the consensus path entirely.

5.1 Trigger Conditions

Phase 3 activates when:

1. CRQCs demonstrably break elliptic curve cryptography in practice.
2. OR: the classical signature adds no security value (all realistic adversaries have quantum access).
3. AND: >99% of network participants have upgraded to Phase 2+ software.

5.2 Changes from Phase 2

Component	Phase 2	Phase 3
Per-block consensus	ML-DSA primary + BLS fallback	ML-DSA only
EC keys	Required (EVM compat)	Optional (legacy EVM only)
BLS keys	Required (fallback)	Deprecated
Block header	∼3,500 B	∼3,400 B (no BLS)
EVM addresses	secp256k1-derived	ML-DSA-derived (new format)

5.3 EVM Address Migration

The most disruptive change in Phase 3 is EVM address derivation. Classical EVM addresses are derived from secp256k1 public keys (keccak256(pubkey)[12 : 32]). Post-quantum addresses must derive from ML-DSA public keys.

Migration path:

1. Users register their ML-DSA public key via a binding transaction signed by their secp256k1 key.
2. The binding creates a mapping: classicalAddress ↔ pqPublicKey.
3. During Phase 3, both address formats are accepted. Transactions may be signed by either key.
4. Eventually, new accounts use only PQ-derived addresses.

6 Key Management During Transition

6.1 Four Key Types

During Phases 1 and 2, validators maintain four keys simultaneously:

Key	Algorithm	Storage	Rotation	HSM Support
EC	secp256k1	Keystore file	Manual	Yes (PKCS#11)
BLS	BLS12-381	Keystore file	Per-epoch capable	Yes (custom)
ML-DSA	ML-DSA-65	Keystore file	Per-epoch capable	Planned (FIPS 140-3)
Pulsar	Module-LWE	DKG shares	Per-epoch (automatic)	N/A (distributed)

6.2 Key Hierarchy

1. The **ML-DSA key** is the validator's long-term identity. It certifies all other keys.
2. The **BLS key** is certified by the ML-DSA key at registration. Rotation requires a new ML-DSA certificate.
3. The **EC key** derives the validator's EVM address. It is bound to the ML-DSA key via a registration transaction.
4. The **Pulsar key** is generated via DKG and rotated automatically each epoch. It is ephemeral.

6.3 Validator Upgrade Path

Existing validators upgrade through three steps:

1. **Generate ML-DSA key pair.** Offline, on validator hardware.
2. **Register ML-DSA public key.** P-Chain transaction signed by the existing EC key, binding the ML-DSA key to the validator's identity.
3. **Upgrade node software.** The new node software signs blocks with both BLS and ML-DSA keys. No downtime required—the upgrade is a rolling restart.

The entire process takes <5 minutes per validator and requires no coordination between validators.

7 NIST Standardization Timeline

Date	Event	Impact on Migration
Aug 2024	FIPS 203/204/205 published	Phase 1 basis established
2025	NIST Round 4 candidates (HQC, BIKE)	Additional KEM options
2025–2026	FIPS 140-3 HSM modules for PQ	HSM support for ML-DSA keys
2027	NSA CNSA 2.0 mandate begins	Government users must deploy PQ
2030	CNSA 2.0 full compliance deadline	Phase 2 trigger (government)
2033+	Estimated CRQC threat window	Phase 3 trigger (if realized)

8 Signature Size Analysis

The practical cost of PQ migration is larger signatures:

Algorithm	Public Key	Signature	Security Level
secp256k1 (ECDSA)	33 B	64 B	128-bit classical
BLS12-381	48 B	96 B (48 aggregated)	128-bit classical
ML-DSA-44	1,312 B	2,420 B	NIST Level 2 (128-bit PQ)
ML-DSA-65	1,952 B	3,309 B	NIST Level 3 (192-bit PQ)
ML-DSA-87	2,592 B	4,627 B	NIST Level 5 (256-bit PQ)
SLH-DSA-128s	32 B	7,856 B	NIST Level 1 (conservative)

ML-DSA-65 signatures are 51.7× larger than ECDSA. Without aggregation, per-block inclusion of N ML-DSA signatures would be prohibitive. STARK aggregation compresses N ML-DSA signatures to ∼200 bytes, making the per-epoch cost independent of validator count.

9 Storage and Bandwidth Impact

Phase	Block Header	Epoch Proof	Annual (headers + epochs)
Phase 1 (current)	144 B	248 B	4.5 TB + 8.1 GB
Phase 2	∼3,500 B	248 B	110 TB + 8.1 GB
Phase 3	∼3,400 B	∼200 B	107 TB + 6.3 GB
Phase 2 (pruned)	∼3,500 B	248 B	9.1 TB (30d) + 8.1 GB

The 24× increase in block header size from Phase 1 to Phase 2 is the primary storage cost. With 30-day pruning (retain only epoch proofs after 30 days), the working storage remains practical.

10 Risk Analysis

Risk	Mitigation	Phase
ML-DSA vulnerability discovered	SLH-DSA fallback (hash-based, conservative)	All
CRQC arrives earlier than expected	Phase 2 can be triggered immediately	$1 \to 2$
HSM vendors lag on PQ support	Software-only key storage with filesystem encryption	1–2
Client upgrade coordination fails	Backward compatibility (old clients verify BLS)	2
EVM address migration causes UX friction	Long parallel period (both formats accepted)	3

11 Conclusion

Post-quantum migration is a process, not an event. The three-phase strategy—hybrid, PQ-primary, pure PQ—allows a production blockchain network to progressively strengthen its cryptographic foundations without coordinated flag-day upgrades. The Lux network's Phase 1 deployment (triple-proof consensus with BLS + ML-DSA + Pulsar) provides hybrid security from genesis. Phases 2 and 3 are defined, with concrete trigger conditions tied to NIST standardization, government mandates, and quantum computing developments. At no point during the migration is the network less secure than it was before—each phase strictly increases the post-quantum security level while maintaining backward compatibility with previous-phase clients.

References

[1] NIST, "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)," August 2024.

[2] NIST, "FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA)," August 2024.

[3] NIST, "FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA)," August 2024.

[4] NSA, "CNSA 2.0: Cybersecurity Advisory on Post-Quantum Cryptography," 2022.

[5] NIST, "IR 8547: Transition to Post-Quantum Cryptography Standards," 2024.

[6] Lux Industries, Inc., "Triple-Proof Quantum Finality: Post-Quantum Consensus for the Lux Network," 2026.

[7] Lux Industries, Inc., "Post-Quantum Cryptographic Suite for EVM," 2024.

[8] Lux Industries, Inc., "Corona: Lattice-Based Threshold Ring Signatures for Anonymous Consensus," 2025.