Adoption Roadmap: From Research Stack to Deployable Infrastructure

Zach Kelling

Lux Industries

2025

Abstract

Research papers describe what is possible; adoption roadmaps describe what happens next. This paper specifies the phased deployment plan for Lux Network's post-quantum and FHE infrastructure, from the current production state (classical BLS consensus with PQ-ready architecture) to full Quasar triple-proof finality with confidential computing. We define four deployment phases with explicit dependencies, migration checkpoints, compatibility layers for each transition, audit milestones, and operator education requirements. Each phase has measurable entry and exit criteria—not aspirational dates, but concrete technical preconditions. The roadmap covers consensus migration (Photon to Quasar), cryptographic primitive rotation (ECDSA to hybrid BLS+ML-DSA), FHE integration (EVM precompiles + T-Chain), and bridge protocol upgrades (Teleport with PQ attestation).

1 Introduction

Lux Network's research program has produced specifications for quantum-secure consensus (Quasar [1]), post-quantum signatures (Corona [2], ML-DSA [3]), fully homomorphic encryption (FHE [4, 5]), and supporting infrastructure (cryptographic agility [6], hybrid certificates [7], zero-trust operations [8]). Deploying these to a live network with real stake requires a plan that does not break what already works.

This roadmap is organized as four phases. Each phase has:

- **Entry criteria**: Technical preconditions that must be met before the phase begins.
- **Deliverables**: Specific deployable artifacts.
- **Exit criteria**: Measurable conditions that confirm the phase is complete.
- **Rollback plan**: How to revert if the phase fails.

2 Current State (Phase 0)

Component	Status
Consensus	Lux consensus family (BLS12-381 signing)
Node binary	`luxd` v1.23.x (Go, single binary)
EVM	C-Chain with chain-VM EVM (Zoo, Hanzo, SPC, Pars)
Signatures	ECDSA (legacy), BLS12-381 (active)
Bridge	Teleport with MPC attestation (classical)
FHE	Library implemented, demos passing, not in consensus
PQ	ML-DSA/Corona implemented, not in production signing
Formal verification	Lean4 proofs for consensus safety/liveness

Table 1: Phase 0: Current production state (as of v1.23.23).

3 Phase 1: Hybrid Signatures and Certificate Infrastructure

3.1 Entry Criteria

1. ML-DSA-65 implementation passes NIST KAT (Known Answer Tests).

2. Hybrid certificate enrollment tested on devnet with ≥ 5 validators for ≥ 30 days.
3. Cryptographic agility layer deployed on testnet with algorithm negotiation in ZAP handshake.
4. External audit of ML-DSA and hybrid certificate code completed.

3.2 Deliverables

1. **Hybrid certificates**: Every mainnet validator holds a BLS+ML-DSA certificate [7].
2. **Algorithm negotiation**: ZAP handshake supports hybrid algorithm sets [6].
3. **Key schedule v2**: Q-Chain stores both classical and PQ public keys per validator.
4. **Dual-signed blocks**: Blocks carry BLS signature (required) and ML-DSA signature (optional, for monitoring).

3.3 Exit Criteria

1. 100% of mainnet validators hold hybrid certificates.
2. ML-DSA signatures appear on $\geq 95\%$ of blocks for ≥ 7 days.
3. No consensus disruption during the transition.

3.4 Rollback

Drop ML-DSA extension from certificates. Revert ZAP handshake to classical-only. No state migration required.

4 Phase 2: Quasar Consensus and Triple-Proof Finality

4.1 Entry Criteria

1. Phase 1 exit criteria met.
2. Quasar consensus passes Lean4 safety and liveness proofs [11].
3. Pulsar threshold DKG tested on testnet with ≥ 21 validators for ≥ 60 days.
4. Tamarin model for FROST-BLS and Pulsar verified.
5. Two independent audits of Quasar consensus code completed.

4.2 Deliverables

1. **Q-Chain**: Platform management chain with Quasar consensus, replacing P-Chain.
2. **Triple-proof finality**: Blocks require BLS aggregate + Pulsar threshold + ZK identity proof.
3. **Validator migration**: Existing P-Chain validators re-register on Q-Chain with new key material.
4. **Slashing**: Post-quantum slashing conditions (double-sign, missing PQ cert).

4.3 Exit Criteria

1. Q-Chain producing blocks with triple-proof certificates for ≥ 30 days.
2. Finality latency $\leq 100\,\text{ms}$ (CPU BLS) or $\leq 10\,\text{ms}$ (GPU BLS) sustained.
3. No safety violations (conflicting finalized blocks).
4. P-Chain deprecated (read-only mode for historical queries).

4.4 Rollback

Revert to P-Chain consensus. Q-Chain state is discarded. Validators re-register on P-Chain with existing keys. Requires coordinated restart.

5 Phase 3: FHE Integration and Confidential Computing

5.1 Entry Criteria

1. Phase 2 exit criteria met.
2. FHE library benchmarks meet SLOs [5] on validator hardware.
3. EVM precompile gas metering verified by Halmos symbolic execution.
4. T-Chain (ThresholdVM) tested on testnet with threshold decryption for ≥ 30 days.
5. One external audit of FHE EVM precompiles completed.

5.2 Deliverables

1. **FHE EVM precompiles**: Encrypted arithmetic, comparison, and bitwise operations available to Solidity contracts on C-Chain and chain-VM EVMs.
2. **T-Chain**: ThresholdVM providing public parameter distribution, ciphertext registration, and threshold decryption.
3. **fhed integration**: FHE daemon deployable alongside validator nodes with mDNS discovery.
4. **Confidential token standard**: Encrypted ERC-20 using `@luxfi/contracts/FHE.sol`.

5.3 Exit Criteria

1. FHE precompiles available on mainnet C-Chain.
2. At least one confidential token deployed and operational.
3. T-Chain threshold decryption operational with $\geq$ 15-of-21 threshold.
4. No gas metering exploits (underpriced FHE operations).

5.4 Rollback

Disable FHE precompiles via network upgrade (set activation timestamp to far-future). T-Chain stops processing new requests; existing ciphertexts remain encrypted. No fund loss—encrypted balances are unspendable until FHE is re-enabled.

6 Phase 4: Full Stack and Ecosystem

6.1 Entry Criteria

1. Phase 3 exit criteria met.
2. Bridge protocol upgraded with PQ attestation (Teleport v2).
3. HSM integration tested with ≥ 3 HSM vendors [9].
4. Operator education program completed for $\geq 80\%$ of validator operators.

6.2 Deliverables

1. **Teleport v2**: Cross-chain messaging with PQ-attested MPC signatures.
2. **HSM support**: Production HSM integration for BLS and ML-DSA signing.
3. **FHE applications**: Dark pool, compliance, blind auction demos running on mainnet.
4. **SDK updates**: `@luxfhe/v2-sdk` with T-Chain integration.

6.3 Exit Criteria

1. End-to-end PQ security from source code (signed releases [10]) to consensus (Quasar) to confidential computing (FHE) to cross-chain (Teleport v2).
2. Zero critical findings in red-team exercise [11].

7 Dependency Graph

```
Phase 0 (Current)
  |
  v
Phase 1 (Hybrid Signatures)
  |  Depends on: crypto-agility, hybrid-certs, ML-DSA audit
  v
Phase 2 (Quasar Consensus)
  |  Depends on: Phase 1, Lean4 proofs, Pulsar DKG, 2 audits
  v
Phase 3 (FHE Integration)
  |  Depends on: Phase 2, FHE benchmarks, Halmos verification
  v
Phase 4 (Full Stack)
     Depends on: Phase 3, Teleport v2, HSM integration
```

Each phase depends on the prior phase's exit criteria, not on a calendar date.

8 Operator Education

Each phase includes documentation and training for validator operators:

Phase	Operator Action Required
Phase 1	Generate ML-DSA keys, update staking registration
Phase 2	Participate in Pulsar DKG, verify Q-Chain migration
Phase 3	Deploy fhed sidecar, configure FHE parameters
Phase 4	Integrate HSM, verify PQ attestation

Table 2: Operator actions per phase.

9 Conclusion

A roadmap is a sequence of verifiable transitions, not a wish list. Each phase in Lux's adoption plan has concrete entry criteria (technical preconditions), measurable exit criteria (production validation), and a rollback plan (if the phase fails). The dependencies are explicit: Phase 2 cannot begin until Phase 1's exit criteria are met, regardless of calendar pressure. This structure ensures that the research stack described in Lux's 55+ papers becomes deployable infrastructure without compromising the security guarantees that the research established.

References

[1] Kelling, Z. (2025). *Quasar: Quantum-Secure Multi-Engine Consensus with Triple-Proof Quantum Finality*. Lux Industries Research.

[2] Lux Industries. *Corona: Two-Round Module-LWE Threshold Signatures*. Lux Industries, 2026. `github.com/luxfi/corona`. Module-LWE (Ringtail-derived), two-round.

[3] Kelling, Z. (2024). *Post-Quantum Cryptographic Suite for Blockchain Infrastructure*. Lux Industries Research.

[4] Kelling, Z. (2025). *FHE API and Developer Model for Practical Private Applications*. Lux Industries Research.

[5] Kelling, Z. (2025). *FHE Benchmarking, Cost Models, and Operational SLOs*. Lux Industries Research.

[6] Kelling, Z. (2024). *Cryptographic Agility Architecture for Long-Lived Blockchain Systems*. Lux Industries Research.

[7] Kelling, Z. (2024). *Hybrid Certificate Chains and Post-Quantum Trust Anchors*. Lux Industries Research.

[8] Kelling, Z. (2025). *Zero-Trust Validator Operations and Service Identity*. Lux Industries Research.

[9] Kelling, Z. (2025). *Secure Enclave, HSM, and Threshold Boundary Design*. Lux Industries Research.

[10] Kelling, Z. (2025). *Signed Software, Reproducible Builds, and Quantum-Resilient Release Pipelines*. Lux Industries Research.

[11] Kelling, Z. (2025). *Security Proof Obligations, Red-Team Methodology, and Verification Strategy*. Lux Industries Research.