The Lux Network

A Regulated, Post-Quantum Blockchain for Digital Securities, Real-World Assets, and Compliant Global Payments

Zach Kelling

Lux Industries

Original: January 1, 2020 | Revised: February 2026

Abstract

We present **Lux**, a regulated post-quantum blockchain network for the issuance, custody, and transfer of digital securities, real-world assets, and compliant payments. Lux launches with a proof-of-NFT validator set of **100 gated slots** operated under an Isle of Man Class 8 Money Transmitter License (CDAX [1]), combining the transparency of public blockchain with the regulatory assurance of a licensed financial institution. The network is designed from the outset to be quantum-resistant via lattice-based cryptography, to support decentralized identity (DID) and integrated anti-money laundering (AML) compliance, and to bridge trustlessly to existing chains through multi-party threshold signing. This document describes the founding architecture, the eight guiding principles, the validator economics, the regulatory framework, and the technical roadmap for the Lux Network as of its launch on January 1, 2020.

Contents

1 Introduction **3**

2 Founding Principles **3**

3 Network Architecture **4**
3.1 The Three Core Chains 4
3.2 Application Chains 4
3.3 Consensus 4

4 The 100 Validator Network **4**
4.1 Design Rationale 4
4.2 Proof-of-NFT Gating 5
4.3 Staking and Rewards 5

5 Regulatory Framework **5**
5.1 Isle of Man Money Transmitter License 5
5.2 Identity Chain and DID 5
5.3 Automated KYC/AML 6

6 Digital Securities and Real-World Assets **6**
6.1 Security Token Standard 6
6.2 Real-World Asset Tokens 6
6.3 Treasury Token 6

7 Interoperability **7**

8 Post-Quantum Cryptography **7**

9 Roadmap **7**

10 Conclusion **8**

1 Introduction

The blockchain industry stands at an impasse. Public blockchains (Bitcoin, Ethereum) offer transparency and permissionless access but cannot issue regulated financial instruments without violating securities laws. Permissioned chains (Hyperledger, R3 Corda) satisfy regulators but abandon the neutrality and composability that make public blockchains valuable. Centralized exchanges (MtGox, Bitfinex, Coincheck) combine the worst of both: regulatory exposure without user custody [3]. Users have lost more than 980,000 BTC (approximately USD 40 billion at current rates) to exchange hacks since 2011.

Lux is designed to resolve this impasse. By operating under an Isle of Man money transmitter license while retaining non-custodial key management, open validator participation (subject to KYC/AML), and public transaction auditability, Lux offers a blockchain that is *simultaneously* regulated and decentralized. The network's hundred-validator founding set is both small enough to operate under a coherent compliance regime and large enough to resist the centralization risks that have plagued purely federated designs.

Lux addresses three additional concerns that existing blockchains do not handle well:

- **Quantum resistance**: Shor's algorithm breaks ECDSA and RSA on a sufficiently large quantum computer. Lux adopts lattice-based primitives (from the `luxfi/lattice` library, based on CKKS [4] and BFV [5]) at every layer that touches user funds.
- **Regulatory compliance**: Lux integrates KYC/AML at the protocol layer via the Identity Chain (I-Chain) and the Decentralized Identifier (DID) specification. No unregistered security is issuable on the network.
- **Interoperability**: Lux bridges to existing blockchains through multi-party threshold signatures (MPC) [6], providing cross-chain liquidity without trusted custodians.

2 Founding Principles

The architecture of Lux is guided by eight principles. These are not marketing statements—they are constraints on the solution space, each of which can veto any proposed change to the network.

1. **Approachability**: Anyone should be able to build on Lux. APIs and libraries target multiple languages (Go, TypeScript, Python) with identical semantics.
2. **Availability**: A financial system that is intermittently available is not a financial system. Lux targets five-nines RPC availability through multi-region validators and leaderless consensus.
3. **Composability**: Small, modular primitives that assemble into larger systems. Every chain, VM, and precompile is usable independently or in combination.
4. **Flexibility**: Well-defined extension points (custom VMs, pluggable consensus, per-chain genesis) with exactly one way to use each.
5. **Longevity**: Bets that will still be correct in a decade. Lattice cryptography over RSA. UTXO where quantum resistance matters. Leaderless over leader-based consensus.
6. **Interoperability**: A chain that cannot communicate with other chains is a database with extra steps. Native cross-chain messaging and threshold-signed bridges.
7. **Security**: Defense in depth. Post-quantum signatures at consensus. Threshold cryptography for key management. Formal verification of the core protocol.
8. **Scalability**: Horizontal chain creation, parallelized EVM execution, and a DAG-based consensus structure that does not serialize all transactions through a single leader.

These principles are developed in depth in a companion document, the *Ethos of Lux* [13].

3 Network Architecture

3.1 The Three Core Chains

Lux is organized as a multi-chain platform. The three core chains are the Platform Chain (P-Chain), the Quantum Chain (Q-Chain), and the Zero-Knowledge Chain (Z-Chain).

P-Chain (Platform) Manages the validator set, staking, rewards, and chain creation. Uses BLS12-381 aggregate signatures for block finality. This is the coordination layer of the network.

Q-Chain (Quantum) Manages post-quantum threshold signatures via Corona (Module-LWE threshold sigs [7]) and ML-DSA [8]. Q-Chain is where the network's quantum-resistant cryptographic state lives.

Z-Chain (Zero-Knowledge) Manages shielded transactions and privacy-preserving smart contracts through zero-knowledge proofs. Shielded payments, private security token transfers, and compliant confidential orders live here.

Together, P, Q, and Z form the **PQZ stack**: the Platform chain coordinates, the Quantum chain provides post-quantum cryptographic finality, and the Z chain provides privacy. Block finality combines attestations from all three: a block is final when it carries a valid BLS aggregate (P-Chain), a valid Pulsar threshold signature (Q-Chain), and a valid ZK proof of consistency with prior state (Z-Chain).

3.2 Application Chains

Application developers deploy sovereign L1 chains via the P-Chain. Each chain chooses its own VM, validator set, genesis parameters, and regulatory configuration. A bank issuing tokenized treasuries runs a different chain from a gaming studio issuing NFTs; they share the P-Chain's security and the Q/Z-Chains' cryptographic primitives without interfering with each other.

At launch, Lux supports the following VM types:

- **EVM** (C-Chain): Ethereum-compatible execution with additional precompiles for PQ signatures, FHE, and threshold verification.
- **XVM** (X-Chain): UTXO-based asset exchange chain. Inherently quantum-resistant through address hashing.
- **Custom**: Any application developer can define their own VM via the Chain VM interface.

3.3 Consensus

Lux uses a family of related consensus protocols—collectively known as *Lux Consensus*—that share a common structure: probabilistic metastable voting, DAG-based transaction ordering, and leaderless finality. The protocol family is named after physical phenomena: *Photon*, *Wave*, *Flare*, *Focus*, *Horizon*, *Ray*, *Nova*, *Nebula*, *Prism*, and *Quasar*. Quasar [10] is the composite protocol that binds P-Chain BLS signatures, Q-Chain Corona/ML-DSA threshold signatures, and Z-Chain ZK proofs into a single triple-proof finality guarantee.

The consensus protocol achieves sub-second finality with no leader election. A block is considered final when it has accumulated attestations from at least $\frac{2n}{3} + 1$ validators across all three core chains. The mathematical treatment is developed in LP-020 [10] and the accompanying protocol papers.

4 The 100 Validator Network

4.1 Design Rationale

Lux launches with a **capped set of 100 validators**. This is neither a permissioned consortium (which lacks sufficient decentralization) nor an unbounded proof-of-stake set (which cannot be operated under a coherent regulatory license). It is a carefully calibrated middle ground: large

enough that no small coalition can seize control, small enough that every validator can be individually verified and licensed.

The 100-slot constraint is enforced by the protocol at the P-Chain layer and cannot be bypassed without an on-chain governance vote requiring two-thirds of the existing validator set.

4.2 Proof-of-NFT Gating

Each of the 100 validator slots corresponds to a unique **Validator NFT** (ERC-721 on the C-Chain, with equivalents on other VMs). Ownership of a Validator NFT is a prerequisite for running a validator node. The NFTs are transferable, but every transfer triggers a re-evaluation of the new holder's KYC/AML status via the Identity Chain (Section 5).

This mechanism produces a regulated-yet-decentralized validator market:

- Anyone can *buy* a Validator NFT on the open market.
- Only KYC/AML-verified entities can *operate* the corresponding validator.
- Slashing is enforced by burning a portion of the NFT-bound stake, with the NFT itself remaining with the operator but losing staking eligibility until restaked.
- A bad actor who buys a Validator NFT but fails KYC loses the right to operate but retains the right to sell the NFT to a compliant operator.

This design is the origin of the *proof-of-NFT* terminology used throughout Lux consensus literature.

4.3 Staking and Rewards

Validators stake LUX tokens in addition to holding a Validator NFT. The minimum stake is set at genesis and adjustable via governance. Rewards accrue proportionally to stake and uptime, with penalties for downtime and slashing for double-signing or equivocation.

The reward curve is designed to incentivize long-term validator commitment: validators who operate continuously for twelve months receive a *commitment bonus* of 5–15% on accumulated rewards, paid at the end of each commitment period.

5 Regulatory Framework

5.1 Isle of Man Money Transmitter License

Lux operates the network's custodial and gateway functions under a **Class 8 Money Transmitter License** issued by the Isle of Man Financial Services Authority [2, 1]. This class of license authorizes bureau-de-change operations, payment services, cheque cashing, and—critically for Lux—the issuance of electronic money backed by real-world assets (Digital Safekeeping Receipts, or D-SKRs).

The Isle of Man jurisdiction was selected for three reasons:

1. **Clear legal status for digital assets**: Manx law treats cryptocurrency as property for transfer purposes and money for transmitter licensing purposes, providing the clearest regulatory basis for token issuance.
2. **EU and UK access via equivalence**: Isle of Man financial licenses enjoy mutual recognition with significant European and UK regulatory regimes.
3. **Sophisticated regulator**: The IOMFSA has been issuing digital-money licenses since 2015 and has a track record of principled, technically competent supervision.

5.2 Identity Chain and DID

The Identity Chain (I-Chain) stores Decentralized Identifier (DID) records and verifiable credentials for every regulated participant on the network. A participant's DID contains:

- A unique on-chain identifier (not derivable from the participant's personal data).
- Verifiable credentials issued by KYC providers, each with a cryptographic attestation and an expiry date.
- A revocation pointer that allows a KYC provider to revoke a credential on-chain if the participant's status changes.
- An accredited-investor flag (for US participants) or equivalent jurisdictional flags.

A smart contract that requires regulated transfers (e.g., a security token) queries the I-Chain before permitting any transfer. If the sender or recipient's DID does not carry a valid credential for the relevant jurisdiction, the transfer reverts.

5.3 Automated KYC/AML

KYC/AML checks occur at three layers:

1. **Onboarding**: A new participant registers via a KYC provider (multiple providers are supported; the network is not beholden to any single vendor). The provider issues a verifiable credential to the participant's DID on the I-Chain.
2. **Transaction**: Every regulated transfer queries the I-Chain to confirm that both parties hold valid credentials.
3. **Ongoing**: KYC providers monitor their issued credentials for sanctions list changes, adverse media, and other ongoing screening events. A provider can revoke a credential at any time, immediately blocking the corresponding participant from further regulated transfers.

6 Digital Securities and Real-World Assets

6.1 Security Token Standard

Lux defines a security token standard (later formalized as LP-001 [11]) that extends ERC-20 and ERC-1404 [9] with:

- Compliance hooks that query the I-Chain on every transfer.
- Corporate actions (dividends, splits, buybacks) as native token operations with automatic pro-rata distribution.
- Transfer restrictions (Regulation D resale windows, accredited investor requirements, jurisdictional blocks).
- A transfer agent role backed by a Class 8 licensed custodian.

6.2 Real-World Asset Tokens

Lux supports the tokenization of physical assets (gold, silver, oil, gas, uranium, real estate) via a combination of custodial attestations and on-chain proofs of redemption. Each RWA token is backed 1:1 (or over-collateralized) by the underlying asset held in a qualified custodian's vault. The custodian posts periodic attestations to the I-Chain; a holder can redeem the token for the underlying asset through a regulated redemption contract.

6.3 Treasury Token

The Lux Treasury Token represents digitized shares of a registered investment company formed pursuant to the Investment Company Act of 1940. Unlike traditional mutual funds, the Treasury Token is closed-end with frequent redemption periods, enabling both peer-to-peer transfer and on-exchange trading.

7 Interoperability

Lux bridges to existing blockchains through the **Lux Bridge**, a non-custodial cross-chain protocol based on multi-party threshold signing. A group of MPC signers, themselves drawn from the Lux validator set, collectively control a multisig on each destination chain. The MPC protocol (CGGMP21 for ECDSA secp256k1, FROST for Ed25519) ensures that no single signer ever holds the full private key, and the threshold t of n is set high enough that no small coalition can seize bridge funds.

Cross-chain transfers are settled via atomic swap: the user locks assets on the source chain, an MPC-signed proof is posted to the destination chain, and the user receives the equivalent wrapped asset. Reverse transfers burn the wrapped asset and unlock the original.

8 Post-Quantum Cryptography

Lux is designed to remain secure against an adversary with access to a large-scale quantum computer. Every primitive that touches user funds uses a post-quantum or quantum-reducible scheme:

- **Signatures**: BLS12-381 (classical, for aggregation efficiency), ML-DSA-65 (FIPS 204 [8], the primary PQ signature), and Corona [7] (Module-LWE threshold signatures, for consensus).
- **Key encapsulation**: ML-KEM-768 (FIPS 203) for confidential channels, with X-Wing hybrid (X25519 + ML-KEM-768) for age-based file encryption.
- **Homomorphic encryption**: TFHE boolean-gate bootstrapping for encrypted computation, CKKS for approximate arithmetic on encrypted data. Both are built on the `luxfi/lattice` library.
- **Zero-knowledge proofs**: Groth16 and PlonK over BN254, with migration planned to P3Q (P3Q; `luxfi/p3q`) for quantum-resistant proof systems.

The detailed cryptographic specification is developed in LP-305 [12].

9 Roadmap

The founding roadmap for the Lux Network is organized in phases:

Phase 1: Genesis (Q1–Q2 2020) Launch the P/Q/Z-Chains with the 100 Validator NFT set. Bring the Isle of Man MTL license online. Issue the first regulated security tokens. Deploy the I-Chain DID registry.

Phase 2: Bridges (Q3–Q4 2020) Launch the Lux Bridge with MPC threshold signing. Support Bitcoin and Ethereum as the first external chains. Add atomic-swap support for wrapped BTC and wrapped ETH.

Phase 3: Exchange (2021) Launch the Lux Exchange (LX), a non-custodial social trading DEX with permission-mapped liquidity aggregators, copy trading, and people-based portfolios. Add ZK-protected order flow to prevent front-running.

Phase 4: RWA (2022–2023) Expand RWA tokenization to precious metals, energy, and real estate. Launch the MChain, a regulated sub-chain for Real-World Asset tokens with integrated SWIFT MT-760/MT-799 asset verification.

Phase 5: Quantum Readiness (2023–2024) Deploy post-quantum signatures across the entire network. Integrate FHE for private smart contracts. Launch the Quantum Safe Financial System.

Phase 6: Scale (2025+) GPU-accelerated EVM for institutional-grade throughput. Formal verification of the core protocol (Lean 4, TLA+, Tamarin, Halmos). Global regulatory footprint expansion beyond the Isle of Man base.

10 Conclusion

Lux is an attempt to resolve a decade-long standoff in blockchain architecture: the trade-off between regulatory compliance and decentralization. Our thesis is that this trade-off is false. A network can be simultaneously regulated (via a coherent jurisdiction and a licensed operator) and decentralized (via an NFT-gated but transferable validator set, non-custodial key management, and public on-chain auditability). The 100-validator design, the PQZ three-chain architecture, the I-Chain compliance registry, and the lattice-based cryptographic foundation are the concrete mechanisms through which this thesis is instantiated.

The principles laid out here are not marketing. They are engineering constraints. Every protocol upgrade, every precompile, every bridge integration is evaluated against them. This is the Ethos of Lux.

References

[1] CDAX Ltd., "Digital Money Issuance and Currency Exchange License (Class 8)," Isle of Man Financial Services Authority. https://www.iomfsa.im/media/2700/1389.pdf.

[2] Isle of Man Financial Services Authority, https://www.iomfsa.im/.

[3] Exchange-hack catalogue (MtGox, Bitfinex, Coincheck, BitGrail et al.), aggregated loss figures compiled from public post-mortems, 2011–2019.

[4] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic Encryption for Arithmetic of Approximate Numbers," *ASIACRYPT*, 2017.

[5] J. Fan and F. Vercauteren, "Somewhat Practical Fully Homomorphic Encryption," IACR ePrint 2012/144, 2012.

[6] Y. Lindell, "Fast Secure Multiparty ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody," *ACM CCS*, 2018.

[7] *luxfi/corona*: Module-LWE threshold signature scheme (Ringtail-derived). https://github.com/luxfi/corona.

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

[9] R. Graves et al., "ERC-1404: Simple Restricted Token Standard," Ethereum EIP, 2018.

[10] Z. Kelling, "LP-020: Quasar — Quantum-Secure Multi-Engine Consensus with Triple-Proof Quantum Finality," Lux Industries.

[11] Z. Kelling, "LP-001: Digital Securities Standard," Lux Industries.

[12] Z. Kelling, "LP-305: Quantum Secure Assets — A Pioneering Methodology for Lux Network in a Post-Quantum Age," Lux Industries.

[13] Z. Kelling, "The Ethos of Lux — Eight Principles for a Durable Blockchain Platform," Lux Industries.

[14] *luxfi/lattice*: Lattice-based cryptographic primitives (CKKS, BFV, TFHE). https://github.com/luxfi/lattice.

[15] *luxfi/papers*: Lux research paper archive. https://github.com/luxfi/papers.