



LP-306: LX — Decentralized Social Trading Exchange

From the 2022 Whitepaper to
the Lux DEX Production Stack

Zach Kelling

Lux Industries

Original: August 2022 | Revised: March 2026

Abstract

LX was proposed in 2022 as a decentralized social trading platform combining copy trading, people-based portfolios, atomic swaps, and a DAO-governed liquidity protocol on the Lux Network. This paper preserves the original design, maps each component to its current implementation status across the Lux DEX (`luxfi/dex`), Lux CEX (`luxfi/cex`), Lux Broker (`luxfi/broker`), and the Lux ATS (`luxfi/ats`), and identifies the features that shipped, evolved, or were superseded by superior alternatives.

Contents

1	Introduction	3
2	Architecture: 2022 Design vs. 2026 Implementation	3
2.1	Matching Engine	3
2.2	Social Trading and Copy Swaps	3
2.3	Decentralized Liquidity Pool	3
2.4	Atomic Swaps and Bridge	4
2.5	Governance and DAO	4
2.6	Security	4
3	Tokenomics: 2022 Model vs. Current	4
4	Features: Shipped, Evolved, Dropped	5
5	The Centralization Problem: 2022 to 2026	5
6	Remaining Roadmap	5
7	Conclusion	5

1 Introduction

The 2022 LX whitepaper described a social trading DEX with the following thesis: centralized exchanges are single points of failure (citing MtGox, Bitfinex, Coincheck); decentralized alternatives at the time (EtherDelta, 0x Protocol) suffered from latency, poor UX, and front-running. LX proposed to solve both with a non-custodial, zero-knowledge encrypted orderbook on a high-throughput L1.

Four years later, the Lux Network ships three exchange-layer components that realize this vision:

Component	Repo	Throughput
Lux DEX (native orderbook)	<code>luxfi/dex</code>	104–250M fills/s (GPU)
Lux CEX (compliance gateway)	<code>luxfi/cex</code>	FIX 4.4 + REST + WS + ZAP
Lux Broker (16-venue SOR)	<code>luxfi/broker</code>	Smart order routing

2 Architecture: 2022 Design vs. 2026 Implementation

2.1 Matching Engine

2022: C++ matching engine compiled to Solidity WASM, running on a Lux L1 chain. Order book stored on-chain.

2026: Multi-engine architecture (`luxfi/dex`): Go (default), C++ (high-freq), Rust (safety-critical), MLX (Apple Silicon). CLOB matching with AMM fallback. Clearinghouse with margin and liquidation. Cross-chain gateway bridging 8 chains. The GPU CLOB kernel sustains 104–126M byte-exact `uint256` fills/s on an NVIDIA GB10 (6.9 ns/match) and roughly 250M fills/s on an Apple M4 Max (4.15 ns/match); the throughput lever is a Knuth Algorithm-D division that replaces a 512-iteration bit-serial `uint256` VWAP ($\sim 8\times$), with output byte-identical to the CPU oracle (LP-203).

2.2 Social Trading and Copy Swaps

2022: Permission-mapped liquidity aggregator smart contracts allowing expert traders to manage investor capital on-chain while investors retain key custody. People-Based Portfolios (PBPs) with transparent performance stats.

2026: The Lux ATS (`luxfi/ats`) implements the regulated version: SecurityToken deployments via `luxfi/standard` on the Lux EVM, portfolio management via the exchange frontend (`luxfi/exchange`), and social trading features (leaderboards, copy-trade, rebalancing). The permission-mapping concept was absorbed into the MPC wallet architecture: users sign with their WebAuthn key share, the ATS co-signs after compliance checks, and capital never leaves the user’s on-chain wallet.

2.3 Decentralized Liquidity Pool

2022: Uniswap V3-style concentrated liquidity with up to 4000x capital efficiency, extended to support both fungible and non-fungible assets in a single pool.

2026: The Lux DEX implements a native orderbook (CLOB) rather than an AMM-only model. AMM pools exist as fallback liquidity via `luxfi/standard/contracts/amm/` (AMM V1–V4, Oracle-Mirrored AMM). The NFT liquidity pool concept was not pursued — the market moved toward orderbook-based NFT trading (Blur/Tensor model) rather than AMM curves for non-fungibles.

2.4 Atomic Swaps and Bridge

2022: HTLC-based atomic swaps with BTC, subsidized by gateway deposits. Cross-chain interoperability via oracles (Chainlink).

2026: The Z-Chain (zero-knowledge bridge) uses homomorphic encryption for shielded cross-chain transfers. The Lux DEX cross-chain gateway supports 8 chains natively. `luxfi/standard/contract/` implements the Warp Messenger protocol for L1↔L2 asset movement. Chainlink oracles replaced with Lux Oracle (native, threshold-signed price feeds).

2.5 Governance and DAO

2022: LUX token governance with quadratic voting, holographic consensus, proof-of-humanity biometric authentication, proxy voting, and Ricardian contracts.

2026: DAO governance contracts exist in `luxfi/standard/contracts/dao/` and `contracts/governance/`. Voting is on-chain with LUX staking. Quadratic voting and proof-of-humanity were not implemented — standard token-weighted voting with delegation is the current model. Ricardian contracts were superseded by on-chain compliance gates (`IComplianceGate` interface).

2.6 Security

2022: SHA-3, PKI, time-delayed multisig, benign fill, hardware wallets for all signing, homomorphic zero-knowledge file systems.

2026: All realized plus post-quantum upgrades:

- SHA-3 → used throughout (Keccak-256 for EVM compatibility, SHA3-256 for non-EVM).
- Multisig → 2-of-3 MPC (CGGMP21 + FROST), strictly superior to multisig (single on-chain address, no n -of- m script complexity).
- Hardware wallets → HSM co-signing (AWS KMS, GCP, Zymbit) for settlement intents.
- Zero-knowledge file system → `PrivateStore.sol` + `/v1/base/private` (E2E encrypted blind blob store, shipped Q1 2026).
- FHE for front-running prevention → FHE CRDT merge (shipped Q1 2026), encrypted orderbook planned for Lux DEX V2.

3 Tokenomics: 2022 Model vs. Current

The 2022 paper proposed an equation-of-exchange valuation model (Burniske: $MV = PQ$; Buterin: $MC = TH$) with an 8% initial inflation decreasing 15% annually to a 1.5% floor, and staking rewards distributed proportionally to validators.

The current Lux Network uses a fixed supply of 10B LUX with no inflation. Validator rewards come from transaction fees, not token emission. The equation-of-exchange model was not adopted — the market moved toward fee-burn models (EIP-1559 style) rather than inflation-funded staking.

The RWA-backed stable currencies (LUXG gold-pegged, LUXU uranium-pegged) described in the 2022 paper remain a design option; deployed stablecoins are USD-backed via registered custodians. (GLUX was the Lux governance token briefly and is unrelated to gold collateral.)

4 Features: Shipped, Evolved, Dropped

2022 Feature	Status	Where
Non-custodial DEX	Shipped	<code>luxfi/dex</code>
Social profiles + stats	Designed	Exchange v2 milestone
Copy trading	Designed	Social trading milestone
People-Based Portfolios	Designed	Portfolio rebalancing milestone
Trading charts	Shipped	Exchange frontend
Indicator alarms	Partial	Webhook events via Hanzo Tasks
Smart search	Shipped	Explorer + exchange search
Watchlist	Shipped	<code>PrivateStore</code> (E2E encrypted)
Content rewards (Steemit)	Dropped	No ROI; social features via standard UX
Trading bots	Shipped	CEX multi-protocol (FIX, WS, ZAP, JSON-RPC)
Token-curated support	Dropped	Standard support model
ETF baskets	Partial	SecurityToken framework supports basket creation
Atomic swaps	Evolved	Cross-chain gateway (8 chains)
Gold-backed stablecoin	Evolved	USDL (USD-backed, not gold)
RWA tokens	Shipped	SecurityToken framework in <code>luxfi/standard</code>
Gateway custodian	Evolved	MPC wallets replace gateway model
Hardware wallet (Yubikey)	Evolved	WebAuthn/passkeys (FIDO2 successor)
DAO governance	Shipped	<code>luxfi/standard/contracts/dao/</code>
Quadratic voting	Dropped	Token-weighted + delegation
Ricardian contracts	Evolved	<code>IComplianceGate</code> on-chain
IEC 61508 / CERT QA	Partial	CI linting + adversarial review (Red/Blue)

5 The Centralization Problem: 2022 to 2026

The 2022 paper catalogued exchange hacks totaling \$40B+ in stolen BTC. The thesis—that centralized custody is the root vulnerability—remains valid. Since 2022, the collapse of FTX (November 2022, \$8B+ in customer losses) dramatically reinforced this point.

Lux’s answer is unchanged: non-custodial MPC wallets where the user holds one key share, the platform co-signs after compliance, and a cold backup enables recovery. No single party can move funds unilaterally. The PostgreSQL ledger is source of truth for trade matching; the chain is source of truth for settlement. If the chain goes down, trades continue; settlement catches up.

6 Remaining Roadmap

1. **Encrypted orderbook:** FHE-encrypted limit orders where the matching engine operates on ciphertexts. Eliminates front-running at the protocol level. Depends on FHE throughput improvements (LP-203, GPU NTT).
2. **Social trading V1:** copy-trade, leaderboards, people-based portfolios. Architecture approved; implementation scoped for Q2 2026.
3. **Cross-chain DEX aggregation:** route orders to external venues via the Lux Broker (16 providers) when on-chain liquidity is insufficient. FINRA 5310 best-execution compliance.
4. **Institutional protocols:** FIX 4.4 gateway (port 8094 on CEX), ZAP binary protocol for internal HFT, post-trade surveillance (wash trading, structuring, velocity detection).

7 Conclusion

The 2022 LX whitepaper proposed a decentralized social trading exchange. Four years later, the core thesis—non-custodial, compliant, high-performance, interoperable—is realized across four

production systems: the Lux DEX (104–250M GPU fills/s native orderbook), the Lux CEX (institutional compliance gateway), the Lux Broker (16-venue smart order router), and the Lux ATS (`luxfi/ats`). The social trading features (copy-trade, PBPs, leaderboards) remain the primary near-term milestone. The encrypted orderbook via FHE is the primary long-term differentiator.

References

- [1] H. Adams, N. Zinsmeister, M. Salem, R. Keefer, and D. Robinson, “Uniswap v3 Core,” 2021.
- [2] J. Nielsen, “F-Shaped Pattern For Reading Web Content,” Nielsen Norman Group, 2006.
- [3] R. Canetti, R. Gennaro, S. Goldfeder, N. Makriyannis, and U. Peled, “UC Non-Interactive, Proactive, Threshold ECDSA with Identifiable Aborts,” *ACM CCS*, 2020.
- [4] J. Faux, “The Crypto Geniuses Who Vaporized a Trillion Dollars,” Bloomberg, 2022.
- [5] M. Herlihy, “Atomic Cross-Chain Swaps,” *PODC*, 2018.