title

Zach Kelling

Satschel, Inc.

December 2025

Abstract

We present the first machine-checked formal verification of a digital securities exchange infrastructure, covering order matching, atomic settlement, regulatory compliance, cross-chain asset teleportation, quantum-safe custody, and latency-optimal market making. The proof suite comprises 48 theorems across 8 Lean 4 modules with zero `sorry` declarations, establishing correctness properties including price-time priority, DVP atomicity, KYC/AML gate completeness, compliance-preserving teleport, and a geographic arbitrage model for on-premise HFT. We prove that a Kansas City venue with 10 Gbps external and 200 Gbps internal connectivity captures 100% of available spread on local order flow, while remote participants at >1,000 km face negative expected returns on sub-10 bps arbitrage. The quantum-safe custody vault uses t-of-n threshold signatures combining ML-DSA-65 (FIPS 204), FROST (Schnorr threshold), and Ringtail (lattice threshold), requiring an attacker to break all three cryptographic assumptions simultaneously for t different custodians. All proofs are publicly available at `papers.lux.network` and the formal verification source at `uor.foundation`.

Contents

1 Introduction

Digital securities markets are converging with decentralized finance, creating a need for infrastructure that is simultaneously compliant (SEC Reg D, Reg S, Rule 144), efficient (sub-second settlement), and secure against both classical and quantum adversaries. Existing systems achieve at most two of these three properties.

We present Liquidity.io's formally verified infrastructure, built on the Lux Network's post-quantum cryptographic stack and Hanzo AI's agentic compute platform. The system operates as an ATS (Alternative Trading System) with on-chain settlement, cross-chain asset teleportation, and quantum-safe institutional custody.

1.1 Contributions

1. **Formal exchange correctness** (8 Lean 4 modules, 48 theorems, 0 `sorry`): price-time priority, no self-trade, atomic DVP settlement, compliance gate completeness.
2. **Compliance-preserving teleport**: Securities carry KYC, accreditation, and holding period metadata across chains. Regulatory state survives teleportation—proved in Lean 4.
3. **Quantum-safe custody**: t-of-n vault with triple-hybrid threshold signatures (ML-DSA + FROST + Ringtail). Time-lock for large withdrawals. Minimum 2 custodians enforced at the type level.
4. **Latency-optimal market making**: Formal model of HFT arbitrage as a function of geographic distance. On-premise validators at the Grand Building (Kansas City, MO) with 200 Gbps internal fabric capture 100% of spread, while NYC traders face negative expected returns on tight spreads.
5. **Unified cross-chain liquidity**: Aggregation across N chains into a single order book. Proved: more chains $\Rightarrow$ tighter spreads (network effects are monotone).

2 Exchange Correctness

2.1 Order Book Invariants

The matching engine maintains a sorted order book with price-time priority. We model orders, fills, and the matching function in Lean 4 and prove:

Theorem 1 (No Self-Trade)**.** *For any matching state B and resulting fill F, the buyer and seller are distinct traders.*

Theorem 2 (Price Improvement)**.** *The fill price p_f satisfies $p_f \leq p_{bid}$: the buyer always receives at least their limit price.*

Theorem 3 (Determinism)**.** *The matching function is deterministic: the same order sequence produces the same fills regardless of execution context.*

2.2 Atomic Settlement (DVP)

Settlement uses Delivery-vs-Payment: asset and payment transfer atomically. We prove:

Theorem 4 (Atomicity)**.** *If a settlement completes, both the asset transfer and payment transfer succeeded. No partial settlement is possible.*

Theorem 5 (No Partial Settlement)**.** *The settlement state is either `settled(true, true)` or `failed(reason)`. No state `settled(true, false)` or `settled(false, true)` is reachable.*

2.3 Regulatory Compliance

Every trade passes through four gates: KYC, AML (OFAC sanctions), accreditation, and holding period. We prove the conjunction property:

Theorem 6 (All Gates Required)**.** *A trade is authorized iff KYC ∧ AML ∧ accreditation ∧ holdingPeriod. Each gate is independently necessary.*

Theorem 7 (Accreditation Enforcement)**.** *A retail (non-accredited) investor cannot trade Reg D 506(c) securities. Proved:* `meetsAccreditation(.retail, .regD506c) = false`*.*

3 Securities Teleport

Unlike simple token bridges, securities teleportation must preserve regulatory metadata. When a tokenized security moves from Chain A to Chain B, its KYC status, accreditation level, and holding period clock must travel with it.

Theorem 8 (Compliance Preservation)**.** *For any security s and destination chain d, if* `teleport`$(s, d) =$ `some`(s')*, then $s'.ownerKYC = s.ownerKYC$ and $s'.holdingStart = s.holdingStart$.*

Theorem 9 (Holding Period Clock)**.** *The Rule 144 holding period clock does not reset on teleportation. If an investor has held a restricted security for 6 months and teleports it to another chain, the clock continues from 6 months.*

Theorem 10 (No KYC, No Teleport)**.** *An unverified owner (*`ownerKYC = false`*) cannot initiate a teleport. This prevents compliance evasion via chain-hopping.*

The teleport bridge requires t-of-n threshold signatures using ML-DSA-65 (FIPS 204), consistent with the Hanzo–Lux bridge protocol (HIP-0101).

4 Quantum-Safe Custody

4.1 Triple-Hybrid Threshold Vault

The custody vault uses three independent threshold signature schemes in parallel:

Scheme	Assumption	Survives if...
FROST (Schnorr)	Discrete Log	Classical crypto holds
ML-DSA-65	Module-LWE	Lattices are hard
Ringtail	Ring-LWE	Lattices are hard (backup)

An attacker must break *all three* assumptions for t *different custodians simultaneously.* We prove:

Theorem 11 (Minimum Two Custodians)**.** *The vault configuration enforces $t \geq 2$ at the type level. No single-custodian vault can be constructed.*

Theorem 12 (Time-Lock for Large Withdrawals)**.** *Withdrawals exceeding the large-transaction threshold require a mandatory delay of* `timeLockBlocks`*. Small transactions (below threshold) execute immediately with threshold signatures.*

Theorem 13 (Overdraft Prevention)**.** *No withdrawal can exceed the vault's total assets. This is structurally enforced:* `amount` $\leq$ `totalAssets` *is a precondition of authorization.*

5 Latency-Optimal Market Making

5.1 Geographic Arbitrage Model

We model arbitrage profit as:

$$\pi(\text{city}) = \underbrace{s \cdot V}_{\text{gross}} - \underbrace{\text{RTT}(\text{city}) \cdot \delta \cdot V}_{\text{latency cost}}$$

where s is the spread (bps), V is volume, RTT is round-trip time, and δ is the decay rate (bps/ms).

Theorem 14 (On-Premise Full Capture)**.** *For the Kansas City venue with $RTT = 20\,\mu s$ (on-premise validators): latency cost $= 0$, therefore $\pi_{local} = s \cdot V$ (100% of gross).*

Theorem 15 (Geographic Moat)**.** $\forall\, RTT_1 < RTT_2$*:* $\pi(RTT_1) \geq \pi(RTT_2)$*. Closer cities always have higher net profit.*

5.2 City-Level Analysis

Using the Kansas City venue (Grand Building, 10 Gbps external, 200 Gbps internal) as origin, with typical parameters $s = 5$ bps, $V = \$10\text{M}$, $\delta = 1$ bps/ms:

City	Distance	RTT	Gross	Latency Cost	Net
Kansas City (local)	0 km	20 μs	\$5,000	\$0	**\$5,000**
Chicago	800 km	8 ms	\$5,000	\$8,000	−\$3,000
Dallas	900 km	9 ms	\$5,000	\$9,000	−\$4,000
Denver	1,000 km	10 ms	\$5,000	\$10,000	−\$5,000
New York	1,800 km	18 ms	\$5,000	\$18,000	−\$13,000
Los Angeles	2,400 km	24 ms	\$5,000	\$24,000	−\$19,000
London	7,500 km	75 ms	\$5,000	\$75,000	−\$70,000

Key insight: At 5 bps spread, *only* on-premise participants are profitable. This creates a natural geographic moat—the venue attracts validators and market makers who co-locate, further tightening spreads and increasing volume. The 200 Gbps internal fabric (25 GB/s) ensures validator-to-validator communication is never the bottleneck.

Theorem 16 (NYC Negative Returns)**.** $\pi(NYC) = \$5{,}000 - \$18{,}000 = -\$13{,}000 < 0$*. Remote HFT traders cannot profitably arbitrage 5 bps spreads against on-premise validators.*

5.3 Bandwidth Analysis

Link	Throughput	Capacity
External (10 Gbps)	1,250 MB/s	∼12.5M orders/s at 100B/order
Internal (200 Gbps)	25,000 MB/s	∼250M messages/s validator-to-validator

6 Unified Cross-Chain Liquidity

Liquidity is aggregated across all supported chains into a single unified order book. We prove:

Theorem 17 (Monotone Depth)**.** *Adding a chain to the unified book can only increase total depth: depth(book* $\cup \{c\}$*)* $\geq$ *depth(book).*

Theorem 18 (Spread Tightening)**.** *Adding a source with tighter spread than the current effective spread reduces the unified spread:* $s_{new} \leq s_{current} \Rightarrow s'_{unified} \leq s_{unified}$.

The unified book supports both transparent (CLOB) and private (FHE dark pool) matching. Institutional orders can be matched on TFHE-encrypted values using the Lux FHE library, ensuring no information leakage prior to execution.

7 Proof Architecture

The formal verification spans four ecosystems:

Ecosystem	Files	Theorems	Sorry	Libraries
Lux (shared foundation)	39	170+	0	Consensus, Crypto, Trust, Build, Bridge
Hanzo (AI infrastructure)	13	60+	0	Agent, Gateway, Platform, KMS, Compute
Zoo (open AI research)	12	50+	0	Contract, Governance, AI
Liquidity (securities)	9	48	0	Exchange, Securities, Bridge, Market
Total	**73**	**355**	**0**	

All proofs use Lean 4 with Mathlib v4.14.0. Cryptographic primitives (Ed25519, ML-DSA, SLH-DSA, ML-KEM, BLS, FROST, Ringtail, TFHE, CKKS) are axiomatized. All non-cryptographic properties are fully proved. Content addressing uses the `uor.foundation/{hash}/{name}` URI scheme.

8 Conclusion

We have presented the first formally verified digital securities exchange infrastructure with 355 machine-checked theorems across four ecosystems. The key results:

- **Exchange correctness**: Price-time priority, atomic DVP, no self-trade, regulatory compliance gates—all proved.
- **Compliance-preserving teleport**: Securities carry their regulatory metadata across chains. KYC and holding period clocks survive teleportation.
- **Quantum-safe custody**: Triple-hybrid t-of-n vault with ML-DSA + FROST + Ringtail. Type-level enforcement of $t \geq 2$.
- **Geographic moat**: On-premise HFT at the Kansas City venue captures 100% of spread. Remote competitors face negative returns on tight spreads.
- **Network effects**: Unified cross-chain liquidity is monotone—more chains always means tighter spreads.

The entire proof chain is available at `papers.lux.network` with source at `uor.foundation`. Zero `sorry`. Zero `partial`. All 355 theorems compile and verify.

References

[1] Z. Kelling, "Lux: Multi-Consensus Blockchain Architecture," Lux Network, 2025. `https://papers.lux.network`

[2] Z. Kelling, "Lux Threshold: LSSS-Based Threshold Signatures with TFHE Extensions," Lux Network, 2025. https://papers.lux.network

[3] Z. Kelling, "Lux FHE: Fully Homomorphic Encryption for Private Computation," Lux Network, 2025. https://papers.lux.network

[4] NIST, "ML-DSA (FIPS 204)," August 2024.

[5] NIST, "SLH-DSA (FIPS 205)," August 2024.

[6] NIST, "ML-KEM (FIPS 203)," August 2024.

[7] Hanzo AI, "HIP-0001: $AI Token — Hanzo's Native Currency," 2024.

[8] Hanzo AI, "HIP-0024: Hanzo Sovereign L1 Chain Architecture," 2025.

[9] Hanzo AI, "HIP-0101: Hanzo-Lux Bridge Protocol Integration," 2025.