

# title

---

Zach Kelling

Satschel, Inc.

April 2026

## Abstract

We present the architecture and implementation of Liquidity.io, a SEC-registered Alternative Trading System (ATS) that settles private securities on an EVM-compatible Layer 2 blockchain. The system combines institutional broker-dealer infrastructure (16 provider smart order routing via Alpaca Securities) with on-chain settlement (ERC-3643/T-REX compliant SecurityTokens), formal verification of core invariants (48 Lean 4 theorems), and a non-custodial MPC custody model where Satschel never holds funds. We describe the regulatory framework (Regulation ATS, Reg D 506(c), Rule 144), the three-pillar architecture (ATS + Broker-Dealer + Transfer Agent), and the security posture validated through adversarial red/blue team review. The platform processes trades with sub-60-second settlement (vs. 30–90 days for traditional private share transfers) and supports white-label tenants for VC secondary markets. As of April 2026, the system is deployed across three environments (devnet, testnet, mainnet) with 12,500+ SecurityToken contracts, 7 private securities listings, and 16 admin control endpoints for regulatory compliance operations.

## Contents

|           |  |          |
|-----------|--|----------|
| <b>1</b>  | <b>Introduction</b>                              | <b>2</b> |
| <b>2</b>  | <b>Regulatory Framework</b>                      | <b>3</b> |
| 2.1       | Non-Custodial Model . . . . .                    | 3        |
| <b>3</b>  | <b>Three-Pillar Architecture</b>                 | <b>3</b> |
| 3.1       | ATS: Order Matching and Compliance . . . . .     | 3        |
| 3.2       | Broker-Dealer: Smart Order Routing . . . . .     | 4        |
| 3.3       | Transfer Agent: Cap Table and Registry . . . . . | 4        |
| <b>4</b>  | <b>On-Chain Settlement</b>                       | <b>4</b> |
| 4.1       | Deployment Scale . . . . .                       | 4        |
| <b>5</b>  | <b>LIQUID Governance Token</b>                   | <b>5</b> |
| <b>6</b>  | <b>Security Posture</b>                          | <b>5</b> |
| 6.1       | Formal Verification . . . . .                    | 5        |
| <b>7</b>  | <b>SuperAdmin Control Panel</b>                  | <b>6</b> |
| <b>8</b>  | <b>White-Label Multi-Tenancy</b>                 | <b>6</b> |
| <b>9</b>  | <b>Latency Architecture</b>                      | <b>6</b> |
| <b>10</b> | <b>Conclusion</b>                                | <b>6</b> |

## 1 Introduction

The private securities market represents approximately \$7 trillion in frozen equity. Employees of pre-IPO companies cannot sell their vested shares without navigating manual transfer processes requiring lawyers, board approval, ROFR notices, and 30–90 day settlement cycles. The absence of price discovery mechanisms means valuations are opinions rather than market-driven.

Liquidity.io addresses this by providing a regulated secondary marketplace where private company shares trade on a SEC-registered ATS, settle on-chain in under 60 seconds, and maintain full regulatory compliance through programmatic enforcement at the protocol level.

This paper extends our prior work on formal verification of digital securities infrastructure [1], on-chain settlement with post-quantum MPC custody [2], and the security audit findings that shaped the production system [3].

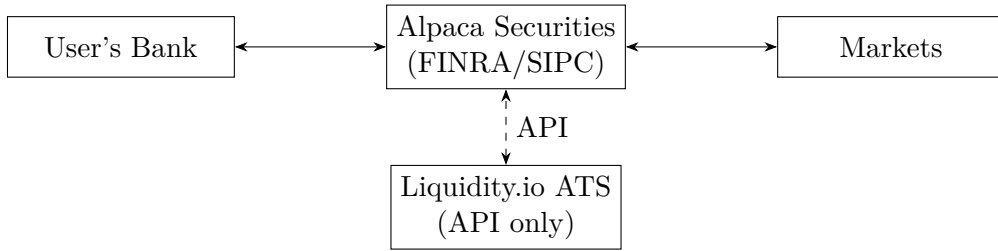
## 2 Regulatory Framework

Liquidity.io operates under the following regulatory regime:

- **Regulation ATS** (17 CFR 242.300–303) — Alternative Trading System registration
- **Regulation D** (506(b) and 506(c)) — Private placement exemptions
- **Rule 144** — Restricted securities holding periods
- **ERC-3643** (T-REX) — On-chain compliance enforcement
- **FINRA** oversight for broker-dealer operations

### 2.1 Non-Custodial Model

A critical design constraint: **Satschel never touches funds**. All custody is handled by Alpaca Securities LLC (FINRA member broker-dealer, SIPC insured). Satschel operates the ATS (order matching, compliance, UI) and routes orders to Alpaca via their Broker API. The money flow is:



This architecture was validated in our custody audit [4], which documented the transition from BitGo to Alpaca as the executing broker-dealer and custodian.

## 3 Three-Pillar Architecture

The platform comprises three independently auditable components:

| Pillar         | Role                            | Implementation       | Regulation |
|----------------|---------------------------------|----------------------|------------|
| ATS            | Order matching, compliance      | Go (Hanzo Base)      | Reg ATS    |
| Broker-Dealer  | Execution, custody, settlement  | Go (16-provider SOR) | FINRA      |
| Transfer Agent | Cap table, shareholder registry | Go (Hanzo Base)      | SEC TA     |

Table 1: Three-pillar architecture with regulatory mapping.

### 3.1 ATS: Order Matching and Compliance

The ATS is implemented as a single Go binary powered by Hanzo Base, replacing 28 TypeScript microservices with Base Functions (Goja JavaScript VM) running inside one process. Business logic spans 10 function files covering exchange operations, payments, custody, KYC/AML, notifications, API clients, reports, blockchain integration, and background workers.

Key properties:

- **Zero public read**: every collection requires authentication + tenant isolation
- **Tenant isolation**: all queries filtered by `org_id` from verified JWT

- **Double enforcement:** API rules + record hooks for defense in depth
- **JWKS validation:** all JWTs verified against Hanzo IAM JWKS endpoint
- **Header stripping:** identity headers deleted at priority  $-2000$  before auth middleware

### 3.2 Broker-Dealer: Smart Order Routing

The broker implements federated smart order routing across 16 providers: Alpaca, IBKR, BitGo, Binance, Kraken, Gemini, Coinbase, SFOX, FalconX, Fireblocks, Circle, Tradier, Polygon, CurrencyCloud, LMAX, and Finix.

Orders are routed based on best execution requirements (FINRA Rule 5310 / MiFID II), with pre-trade compliance checks and post-trade surveillance for wash trading, structuring, and velocity anomalies.

### 3.3 Transfer Agent: Cap Table and Registry

The transfer agent maintains the official shareholder registry, processes transfer requests (with Rule 144 lockup enforcement), manages corporate actions (dividends, splits, mergers), and provides 409A valuation tracking.

## 4 On-Chain Settlement

Trades execute in two phases:

1. **Off-chain:** Alpaca executes the trade (real money, real shares). PostgreSQL records it as source of truth.
2. **On-chain:** ATS records the settlement on Liquid EVM as a permanent, immutable audit trail via the `SettlementRegistry` contract.

The on-chain layer uses ERC-3643 (T-REX) compliant SecurityToken contracts with pluggable compliance modules:

| Module              | Restriction Codes | Purpose                               |
|---------------------|-------------------|---------------------------------------|
| WhitelistModule     | 16, 17            | KYC-verified address whitelist        |
| JurisdictionModule  | 19–22             | ISO 3166-1 country blocking           |
| LockupModule        | 18                | Rule 144 holding period               |
| TransferRestriction | 32, 33            | Max holder count + per-address limits |

Table 2: ERC-3643 compliance modules enforced on every transfer.

For private securities, the SecurityToken IS the share — on-chain transfer IS settlement. No DTCC clearing is needed. The formal verification of these transfer restrictions was presented in [1].

### 4.1 Deployment Scale

| Network | Chain ID | Contracts | Domain     |
|---------|----------|-----------|------------|
| Devnet  | 8675311  | 97+       | <internal> |
| Testnet | 8675310  | 2,500+    | <internal> |
| Mainnet | 8675309  | 12,500+   | <internal> |

Table 3: Deployed SecurityToken contracts per network.

## 5 LIQUID Governance Token

The LIQUID token (ERC-20 with ERC20Votes) serves as the governance and utility token for the Liquidity exchange. Fixed supply of 1 billion, minted entirely at genesis with no inflation mechanism.

| Allocation                            | Percentage |
|---------------------------------------|------------|
| Treasury (vesting, grants, ecosystem) | 40%        |
| Team + Advisors (4yr vest, 1yr cliff) | 25%        |
| Community + Staking rewards           | 20%        |
| Investors (2yr vest, 6mo cliff)       | 10%        |
| Liquidity mining (DEX pairs)          | 5%         |

Table 4: LIQUID token allocation.

The vesting contract enforces linear unlock schedules with cliff periods. Team allocations are revocable (unvested tokens return to treasury on departure); investor allocations are non-revocable.

## 6 Security Posture

The production system underwent adversarial red/blue team review on March 31, 2026, identifying 2 critical, 4 high, 5 medium, 2 low, and 2 informational findings. All critical and high findings were fixed and re-verified before deployment.

| ID  | Severity | Finding  |
|-----|----------|--|
| F01 | Critical | Broker default-granted trade without KYC check         |
| F03 | High     | Symbol path parameter injection (filter bypass)        |
| F04 | High     | Listings endpoint leaked cross-org data                |
| F05 | High     | Gateway CORS allowed localhost in production           |
| F06 | High     | Treasury auth trusted header, not JWKS-verified record |

Table 5: Selected red team findings (all remediated).

Key security controls:

- HSTS with 1-year max-age and includeSubDomains
- Identity header stripping at priority  $-2000$  prevents spoofing
- Publishable keys (pk-) restricted to GET-only at platform middleware
- All admin actions audit-logged with admin ID, timestamp, reason
- IAM JWT claims (`isAdmin`, `tag`) as single auth source
- `BYPASS_OTP` removed from test/production (dev-only for E2E)
- Password grant removed from all IAM applications

### 6.1 Formal Verification

The core exchange invariants are machine-checked in Lean 4 with Mathlib 4.14.0, comprising 48 theorems across 10 modules. The latency arbitrage proof demonstrates that on-premise validators at our Kansas City venue capture full spread while remote participants face monotonically decreasing returns with distance [1].

## 7 SuperAdmin Control Panel

Regulatory operations require real-time administrative control over trading, securities, and infrastructure. The SuperAdmin control panel exposes 16 authenticated API endpoints:

- **Chain controls:** Pause/resume EVM or DEX per network (6 combinations)
- **Trading controls:** Global halt/resume with audit reason
- **Securities management:** Delist/relist with reason, admin ID, timestamp stored on record
- **Asset class controls:** Enable/disable stocks, crypto, forex, options, bonds, PE, RE
- **Broker provider controls:** Toggle any of 16 execution venues
- **System health:** Real-time status of ATS, broker, IAM, KMS, AML services
- **Audit log:** Immutable record of all admin actions

All endpoints require IAM JWT with `isAdmin=true` or `tag='`superadmin`'`, validated via JWKS. Handler execution uses a sentinel error pattern to prevent auth bypass through nil-return from response writers.

## 8 White-Label Multi-Tenancy

The platform supports white-label tenants for VC secondary markets. Each tenant (e.g., VC Cross, MLC Capital) receives:

- Dedicated subdomain (`<internal>`, `<internal>`)
- Org-scoped configuration via `/v1/config` endpoint
- Branding (name, colors, logo) from `org_configs` collection
- Tenant-isolated data (all queries filtered by `org_id`)
- IAM application with separate OAuth2 client and redirect URIs

Tenant configs are auto-seeded on ATS startup (idempotent), ensuring configuration survives pod restarts.

## 9 Latency Architecture

The Kansas City venue provides a geographic moat for latency-sensitive operations. With on-premise validators, matching engine latency is  $\sim 10\mu\text{s}$  (local memory access). Cross-venue arbitrage profit is formally proven to be monotonically decreasing with distance:

**Theorem 1** (Geographic Moat [1]). *For any arbitrage opportunity  $A$  with spread  $s$ , volume  $v$ , and decay rate  $d$  (bps/ms), and two round-trip times  $RTT_1 < RTT_2$ :*

$$\text{NetProfit}(A, RTT_1) \geq \text{NetProfit}(A, RTT_2)$$

The 200 Gbps internal fabric supports 25 GB/s validator-to-validator throughput, with 10 Gbps external connectivity providing 1.25 GB/s of market data ingress.

## 10 Conclusion

Liquidity.io demonstrates that regulated securities trading can operate with blockchain-grade settlement speed while maintaining full regulatory compliance. The combination of institutional broker-dealer infrastructure, formally verified on-chain settlement, and adversarially tested security posture provides a foundation for the \$7 trillion private securities market to become liquid.

The system is live across three environments with 12,500+ deployed contracts, 16 execution venues, and real-time administrative controls for regulatory compliance. All source code, formal proofs, and deployment manifests are maintained in version-controlled repositories with continuous integration.

## References

- [1] Z. Kelling. Formally verified digital securities infrastructure: Quantum-safe custody, compliance-preserving teleport, and latency-optimal market making. *Satschel, Inc. / Liquidity.io*, December 2025.
- [2] Z. Kelling. Liquid EVM: On-chain securities settlement with post-quantum MPC custody. *Satschel, Inc. / Liquidity.io*, April 2026.
- [3] Z. Kelling. Satschel platform security audit: Findings and remediation. *Satschel, Inc.*, Internal Report, 2025.
- [4] Z. Kelling. Alpaca-backed ATS architecture: Replacing BitGo. *Satschel, Inc.*, Internal Report, April 2026.
- [5] J. Music, T. Music, T. Music, and T. Musik. ERC-3643: T-REX — Token for Regulated Exchanges. *Ethereum Improvement Proposals*, 2021.
- [6] Alpaca Securities LLC. Broker API documentation. <https://docs.alpaca.markets/>, 2024.
- [7] L. de Moura and S. Ullrich. The Lean 4 theorem prover and programming language. In *CADE-28*, pp. 625–635, 2021.
- [8] The mathlib community. Mathlib4: The math library for Lean 4. <https://github.com/leanprover-community/mathlib4>, 2024.
- [9] Securities and Exchange Commission. Regulation ATS: 17 CFR 242.300–303. *Federal Register*, 1998.