title

Zach Kelling

Satschel, Inc.

Version 1.0 — April 2026

Abstract

We present **Liquid EVM**, a Layer 2 blockchain purpose-built for digital securities settlement. Operating as a sovereign subnet built on Quasar Consensus, Liquid EVM features 19 post-quantum safe precompiles, threshold MPC custody via CGGMP21 and FROST protocols, and atomic settlement through the USDL stablecoin. The system implements a chain-resilient settlement architecture where PostgreSQL serves as the authoritative source of truth, while on-chain settlement provides cryptographic finality. This design enables the Alternative Trading System (ATS) to continue matching orders even during chain unavailability, with settlement catching up automatically. We describe the complete architecture spanning order matching, compliance gating, MPC signing, and on-chain mint/burn cycles, and analyze the post-quantum security properties of the precompile suite.

1 Introduction

Digital securities—tokenized equities, debt instruments, and alternative assets—require settlement infrastructure that provides both regulatory compliance and cryptographic guarantees. Traditional clearinghouses (DTCC, Euroclear) settle T+1 or T+2 with counterparty risk, opaque processes, and centralized points of failure. On-chain settlement can reduce this to seconds with atomic guarantees, but existing blockchain platforms lack the regulatory primitives and post-quantum security required for institutional adoption.

Liquid EVM addresses this gap as a purpose-built Layer 2 blockchain built on Quasar Consensus. It combines:

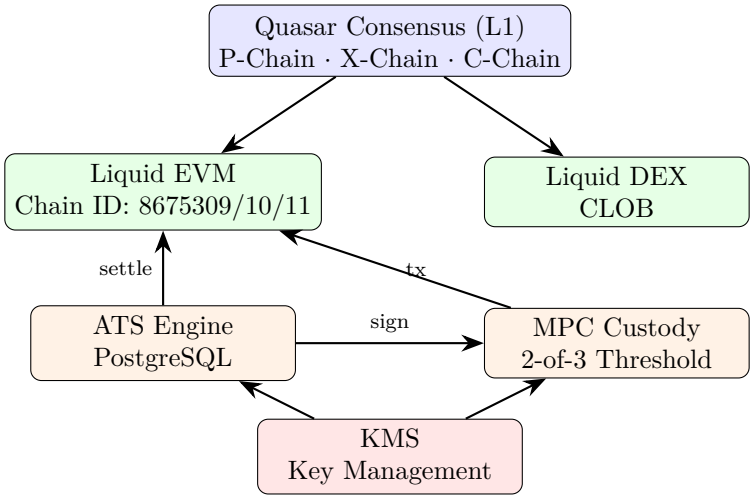
- **19 precompiles** including NIST PQC standards for quantum-resistant cryptography
- **2-of-3 MPC custody** via CGGMP21 (ECDSA) and FROST (EdDSA) for institutional-grade key management
- **Chain-resilient settlement** where trades execute regardless of chain availability
- **Regulatory primitives** for ATS, broker-dealer, and transfer agent compliance
- **USDL stablecoin** as the atomic settlement unit (1:1 USD backed)

The system processes securities trades through a deterministic pipeline: order → compliance check → CEX match → PostgreSQL record → MPC sign → on-chain mint/burn. This paper describes each stage and analyzes the security properties of the complete architecture.

2 Architecture Overview

2.1 Network Topology

Liquid EVM operates as a subnet built on Quasar Consensus, inheriting the base layer's consensus and validator management while maintaining sovereignty over its execution environment.



2.2 Chain Parameters

Parameter	**Devnet**	**Testnet**	**Mainnet**
EVM Chain ID	8675311	8675310	8675309
Network ID	3	2	1
Validators	5	5	5
Native Token	LQDTY	LQDTY	LQDTY
Total Supply	10,000,000,000 (10B)		
Decimals	18		
Block Gas Limit	15,000,000		
Target Block Rate	2 seconds		

Table 1: Liquid EVM chain parameters across environments.

2.3 Token Architecture

Three token types operate on Liquid EVM:

LQDTY Native gas token for transaction fees and validator staking. 10B supply, 18 decimals. WLQDTY (wrapped) extends the standard wrapped-native pattern for DeFi composability.

USDL The sole dollar-denominated stablecoin on the chain. 1:1 backed by USD via ACH/wire deposits through regulated banking rails. Minted on deposit, burned on withdrawal. Not a SecurityToken—implemented as a standard ERC-20.

SecurityToken ERC-20 tokens representing tradable assets (equities, crypto, commodities). Real symbols (AAPL, MSFT, ETH, BTC) collateralized 1:1 by broker holdings at Alpaca, IBKR, and other regulated custodians.

3 Settlement Architecture

3.1 Chain-Resilient Design

The fundamental design principle is that **the ATS never blocks on chain availability**. PostgreSQL is the source of truth for all trade records. On-chain settlement provides cryptographic finality but is asynchronous.

Algorithm 1 Chain-Resilient Settlement

```
User submits order via API
CEX engine matches order (Liquid DEX orderbook, 434M ops/sec)
Trade record written to PostgreSQL (source of truth)
Settlement queued in pending_settlements table
repeat
    Settlement cron (every 30 seconds):
        Fetch batch from pending_settlements
        For each settlement:
            MPC sign transaction (CGGMP21, 2-of-3)
            Submit to Liquid EVM (mint target / burn source)
            If success: mark settled, record tx hash
            If chain down: mark retry, increment counter
until all pending settlements processed
```

3.2 Order Flow

A complete trade lifecycle proceeds through five stages:

1. **Pre-trade compliance**: KYC/AML/sanctions check, offering-type gating (Reg D/S/A+/CF), accreditation verification, investment limit enforcement.
2. **Order matching**: CEX engine routes to DEX orderbook. Unmatched orders route to external venues (Alpaca, IBKR) via the Liquid Broker smart order router.
3. **PostgreSQL record**: Trade recorded with full audit trail. This is the legal record of the transaction.
4. **MPC signing**: Settlement intent created, submitted to MPC service. User's device key + ATS auto-co-sign (after compliance) = 2-of-3 threshold met. HSM co-signing for institutional settlements.
5. **On-chain settlement**: Signed transaction mints target SecurityToken and burns source (USDL for buys, SecurityToken for sells). Atomic—both sides settle or neither does.

3.3 USDL Settlement Mechanics

USDL serves as the atomic settlement unit:

- **Deposit**: User sends USD via ACH/wire → ATS verifies receipt → mints equivalent USDL to user's MPC wallet

- **Buy**: USDL burned from buyer's wallet, SecurityToken minted to buyer's wallet (atomic)
- **Sell**: SecurityToken burned from seller's wallet, USDL minted to seller's wallet (atomic)
- **Withdraw**: USDL burned → ATS initiates ACH/wire to user's bank account

No LUSDC, no LUSDT—USDL is the only dollar on the chain, eliminating fragmentation.

4 MPC Custody Architecture

4.1 Threshold Signature Scheme

Every user receives a 2-of-3 MPC wallet on Liquid EVM:

Participant	Role	Description
User	Key share 1	Device/browser key, biometric-gated (Face ID)
ATS	Key share 2	Auto-co-signs after compliance checks pass
Backup	Key share 3	Cold storage recovery, HSM-protected

Table 2: MPC wallet participants. Any two participants can sign.

CGGMP21 ECDSA (secp256k1): Used for all EVM transactions on Liquid EVM. The CGGMP21 protocol [5] provides identifiable abort and optimal round complexity.

FROST EdDSA (Ed25519): Used for cross-chain transactions (Solana, TON). The FROST protocol [6] provides robustness against malicious signers.

4.2 Biometric Trade Approval

For trades exceeding configurable thresholds, the system requires biometric confirmation:

1. Trade intent created by ATS after order match
2. Push notification sent to user's mobile device (APNS/FCM)
3. User authenticates via Face ID / Touch ID
4. Device key share signs the settlement transaction
5. ATS key share auto-co-signs (compliance already verified)
6. 2-of-3 threshold met, transaction submitted to chain

4.3 Key Management Layers

Three layers of key management provide defense in depth:

KMS (Liquid Threshold): Secrets, certificates, encryption keys. Vault-compatible Transit Engine for encryption-as-a-service. Shamir unseal, HSM backing (PKCS#11). Per-org key isolation.

MPC (Liquid Threshold): Threshold signing for transactions. CGGMP21 + FROST protocols. 2-of-3 or 3-of-5 keygen. Settlement lifecycle management.

HSM Co-signing: AWS KMS, GCP Cloud HSM, Zymbit hardware. Final authorization layer for high-value settlements.

5 Precompile Suite

Liquid EVM activates 19 precompiles at genesis, providing native performance for cryptographic operations that would be prohibitively expensive in EVM bytecode.

Category	Precompile	Address	Standard
Post-Quantum	ML-DSA	`0x0200...06`	FIPS 204
	SLH-DSA	`0x0600...01`	FIPS 205
	ML-KEM	`0x0200...07`	FIPS 203
	PQCrypto	`0x...9003`	Composite
	Blake3	`0x0500...04`	BLAKE3
Threshold	FROST	`0x0800...02`	RFC 9591
	CGGMP21	`0x0800...03`	CGGMP21
	Ringtail	`0x0200...0B`	Ring-CT
Curves	Ed25519	`native`	RFC 8032
	secp256r1	`native`	NIST P-256
	SR25519	`native`	Ristretto
Privacy	FHE	`0x0700...00`	CKKS/BGV
	ZK	`0x0900...00`	Groth16
	HPKE	`0x...9200`	RFC 9180
Privacy	ECIES	`0x...9201`	IEEE 1363a
	Ring	`0x...9202`	Borromean
DeFi	DEX Pool	`0x...9010`	Uniswap v4
	Router	`0x...9012`	Swap Router
Compute	Graph	`0x0500...10`	On-chain GNN

Table 3: Liquid EVM precompile suite. AI Mining is intentionally excluded from Liquid EVM (enabled on Zoo EVM only).

5.1 Post-Quantum Security Analysis

The post-quantum precompiles provide NIST PQC security levels:

- **ML-DSA** (Module-Lattice Digital Signature Algorithm): FIPS 204, Level 3/5 security. Replaces classical ECDSA for long-term key authentication. Signature

size 3.3 KB (ML-DSA-65).

- **SLH-DSA** (Stateless Hash-Based Digital Signature Algorithm): FIPS 205, Level 3/5. Hash-based signatures with minimal cryptographic assumptions. Larger signatures (17 KB) but maximum conservative security.
- **ML-KEM** (Module-Lattice Key Encapsulation Mechanism): FIPS 203, Level 3/5. Quantum-resistant key exchange for establishing shared secrets. Used in MPC key generation ceremonies.

The hybrid approach uses classical ECDSA (secp256k1) for immediate transaction signing while ML-DSA provides a quantum-resistant attestation layer. If ECDSA is broken by a quantum adversary, the ML-DSA attestation remains valid, enabling key migration without fund loss.

6 Regulatory Compliance

6.1 Three-Pillar Architecture

Liquidity operates three regulated entities, each with on-chain enforcement:

ATS (Alternative Trading System): SEC Rule 300-303. Order matching, trade execution, settlement. On-chain: SecurityToken mint/burn, USDL transfers.

Broker-Dealer (BD): FINRA registered. Smart order routing to 16 venues (Alpaca, IBKR, BitGo, Binance, Kraken, etc.). Pre-trade risk checks. Best execution (FINRA 5310).

Transfer Agent (TA): SEC Rule 17Ad. Shareholder record keeping, dividend distribution, transfer restrictions. On-chain: cap table management, restriction enforcement, corporate actions.

6.2 ComplianceGate

The ComplianceGate precompile enforces KYC/AML requirements at the smart contract level:

```
// On-chain compliance check before any SecurityToken transfer
function transfer(address to, uint256 amount) {
    require(ComplianceRegistry.isApproved(msg.sender));
    require(ComplianceRegistry.isApproved(to));
    require(!ComplianceRegistry.isSanctioned(to));
    // Reg CF: check 12-month resale restriction
    require(block.timestamp >= purchaseDate[msg.sender]
            + 365 days);
    super.transfer(to, amount);
}
```

6.3 RegCF Enforcement

Regulation Crowdfunding imposes specific on-chain constraints:

- 12-month resale restriction with FIFO lot tracking
- Investment limits based on income/net worth (on-chain verified via KYC oracle)
- Accreditation checks for 506(b)/506(c) offerings
- Burned tokens excluded from holder statements

7 Deployment Architecture

7.1 Infrastructure

Component	Platform	Cluster	Nodes
L2 Validators	GKE	liquidity-chains	4 nodes
ATS + Services	GKE	liquidity-devnet/test/main	3 nodes each
Quasar L1	DOKS	quasar-validators	8 nodes

Table 4: Infrastructure topology. Quasar L1 on DigitalOcean DOKS, Liquidity L2 on Google GKE. Never mixed.

Each environment namespace runs: 5 validator nodes (StatefulSet), DEX service, Blockscout explorer + frontend, The Graph indexer (graph-node + IPFS), Traefik ingress.

7.2 Liquid Operator

The Liquid Operator is a Rust-based Kubernetes operator managing 18 Custom Resource Definitions:

Chain CRDs (6): LiquidNetwork, LiquidChain, LiquidIndexer, LiquidExplorer, LiquidGateway, LiquidMPC.

Platform CRDs (12): LiquidPlatform, LiquidATS, LiquidBD, LiquidTA, LiquidIAM, LiquidKMS, LiquidIngress, LiquidApp, LiquidCompliance, LiquidDatastore, LiquidKV, LiquidSQL.

7.3 Single Binary Node

The `lqd` binary serves triple duty via self-installing plugin symlinks:

8 Security Analysis

8.1 Threat Model

We consider adversaries with:

- Quantum computing capability (Shor's algorithm for ECDSA, Grover's for hashing)
- Network-level access (MITM, replay attacks)

Algorithm 2 Self-Installing Plugin Node

if env `LUX_VM_TRANSPORT` is set **then**
  if executable name contains DEX VM ID **then**
    Run as DEX VM plugin subprocess
  else
    Run as EVM plugin subprocess
  end if
else
  Install self as symlinks in plugin directory:
    `plugins/<EVM_VMID>` → self
    `plugins/<DEX_VMID>` → self
  Start Quasar node (which discovers plugins)
  Start ZAP binary protocol listener (port 9633)
  Block until shutdown signal
end if

- Compromise of a single MPC key share (1-of-3)
- Access to the ATS database (read-only)

8.2 Defense Layers

1. **Quantum resistance**: ML-DSA/SLH-DSA attestations survive ECDSA compromise. ML-KEM protects key exchange.
2. **Threshold signatures**: Compromising 1-of-3 key shares is insufficient. User + Backup can recover without ATS. ATS + User can transact without Backup.
3. **Chain resilience**: PostgreSQL source of truth means chain compromise cannot forge trade records. Settlement is verification, not authority.
4. **Compliance gating**: On-chain KYC/AML enforcement prevents unauthorized transfers even if keys are compromised.
5. **HSM co-signing**: High-value settlements require hardware security module authorization, adding a physical security layer.

8.3 Comparison with Traditional Settlement

9 Related Work

The Lux Network consensus protocol is described in [1]. Post-quantum precompile design follows [2]. The EVM precompile architecture is detailed in [3]. Zoo EVM [4] shares the same precompile base with the addition of AI Mining for decentralized science applications. The MPC threshold signature protocols are based on CGGMP21 [5] and FROST [6].

Property	DTCC/Clearinghouse	Liquid EVM
Settlement time	T+1 (24 hours)	30 seconds (cron)
Counterparty risk	Central counterparty	Atomic (no counterparty)
Audit trail	Opaque, delayed	On-chain, real-time
Key management	Centralized HSM	2-of-3 MPC + HSM
Quantum resistance	None	NIST PQC Level 3/5
Availability	Business hours	24/7/365
Cross-border	T+2, correspondent banks	Instant, same chain
Transparency	Quarterly reports	Block explorer

Table 5: Liquid EVM vs traditional clearinghouse settlement.

10 Conclusion

Liquid EVM demonstrates that post-quantum safe, regulation-compliant securities settlement is achievable on a Layer 2 blockchain. The chain-resilient architecture—where PostgreSQL is the source of truth and on-chain settlement provides cryptographic finality—eliminates the false dichotomy between reliability and decentralization. The 19-precompile suite provides native-speed access to quantum-resistant cryptography, threshold signatures, and privacy primitives, while the three-pillar regulatory architecture (ATS/B-D/TA) ensures compliance at the protocol level.

The system is live across three environments with 15 validator nodes, processing securities settlements for equities and crypto assets. Future work includes sovereign L1 migration (full sovereign consensus), cross-chain bridge integration with Zoo EVM for DeSci asset interoperability, and expansion of the SecurityToken suite to support derivatives (options, futures, forex) via the `@liquidity/standard` contract library.

References

[1] Kelling, Z. "Quasar Consensus: Multi-Engine Blockchain Consensus." Satschel, Inc., 2025.

[2] Kelling, Z. "EthFalcon: Post-Quantum Cryptography for EVM Chains." Satschel, Inc., 2025.

[3] Kelling, Z. "Lux EVM Precompiles: Native Cryptographic Primitives." Satschel, Inc., 2025.

[4] Kelling, Z. "Zoo EVM: Post-Quantum Safe L2 with AI-Native Precompiles." Zoo Labs Foundation, 2026.

[5] Canetti, R., Gennaro, R., Goldfeder, S., Makriyannis, N., Peled, U. "UC Non-Interactive, Proactive, Threshold ECDSA with Identifiable Aborts." ACM CCS 2020.

[6] Komlo, C., Goldberg, I. “FROST: Flexible Round-Optimized Schnorr Threshold Signatures.” SAC 2020.