

Non-Custodial MPC Custody for a Regulated ATS: ACM’s Threshold-Signing Architecture for Compliant Digital-Securities Trading

ACM Global Tech

Abstract

ACM Global Tech licenses an end-to-end regulated banking and digital-securities stack in which custody is *non-custodial by construction*: no single operator ever holds an investor’s private key. This white paper describes how ACM combines a non-custodial Alternative Trading System (ATS) with multi-party computation (MPC) threshold signing to operate a compliant venue for trading tokenized securities. The architecture derives from the Lux non-custodial ATS design [1], the threshold-custody construction for digital securities [2], and the Hanzo platform integration that supplies identity, key management, gateway, and persistence services [3]. The stack is built on Lux (blockchain, post-quantum cryptography, and FHE), Hanzo (AI and data), and Zen (LLMs), and is delivered to regulated institutions through ACM’s W3A (w3a.foundation) membership, under which ACM licenses this intellectual property and partners to resell and co-build for regulated institutions.

1 The Problem: Custody Risk in Regulated Trading

A regulated securities venue faces a structural tension. To trade and settle, the venue must be able to authorize asset movements; but if the venue holds investor private keys, it becomes a custodian and a single point of catastrophic failure—exposed to insider theft, key compromise, and the heightened regulatory burden of holding customer assets. At the same time, the venue must satisfy securities obligations: operating within SEC Regulation ATS, meeting broker-dealer requirements under the Securities Exchange Act of 1934, and honoring transfer-agent obligations under Section 17A [1]. The challenge is to authorize trades and enforce compliance *without* any single party being able to move an investor’s assets unilaterally.

2 ACM’s Approach

ACM’s regulated-ATS offering composes a non-custodial trading venue with threshold custody so that authorization is always distributed.

Non-custodial ATS.

The venue is architected as a non-custodial ATS for digital securities, compliant with SEC Regulation ATS, broker-dealer requirements, and transfer-agent obligations, in which non-custodial operation is achieved via MPC threshold signing with a 2-of-3 threshold so the platform never holds private keys [1]. Settlement occurs on the Lux EVM with T+0 atomic finality, and securities follow ERC-1400/ERC-1404 contracts with on-chain transfer restrictions [1].

Threshold custody for every wallet.

Each investor wallet is a 2-of-3 threshold address whose shares are split across the user’s device, the operator (which auto-co-signs only after compliance checks), and a cold backup; no party ever holds the complete key [2]. Two complementary protocols cover the relevant chains: CG-GMP21 threshold ECDSA over secp256k1 for EVM-compatible chains, and FROST threshold Schnorr over Ed25519 for EdDSA chains [2]. Shares can be refreshed (reshared) without changing the on-chain address, and an HSM attestation layer co-attests each signing share without weakening unforgeability [2].

Platform services for a regulated workflow.

Identity and investor onboarding (KYC/AML), key management for MPC material, API routing, and data persistence are provided by the Hanzo platform (IAM, KMS, Gateway, Base), as demonstrated by the digital-securities integration that composes these services for a regulated financial application [3].

The composition delivers the security property that matters to regulators and investors alike: because every asset movement requires a 2-of-3 threshold signature, a compromise of the operator alone is insufficient to move assets [1, 2].

A complete banking surface. The regulated-ATS offering sits within ACM’s broader product stack, which includes a Stripe-class payment service provider (PSP) and a full Banking-as-a-Service (BaaS) product. Institutions can therefore adopt custody, trading, payments, and banking as composable parts of a single regulated platform rather than integrating disparate vendors.

Real-time AI/ML for AML. ACM operates a real-time AI/ML anti-money-laundering and transaction-monitoring engine, complementing the KYC/AML onboarding and real-time FINRA trade reporting provided by the platform integration [3]. Suspicious activity is scored as transactions flow, so compliance enforcement is continuous rather than purely point-in-time at onboarding.

3 Cryptographic Foundation

- **Regulated non-custodial venue.** *Non-Custodial Blockchain ATS: Architecture of a Regulatory-Compliant Securities Exchange* [1] presents the ATS architecture as a single Go binary, maps it to SEC Regulation ATS, broker-dealer, and transfer-agent obligations, and specifies the 2-of-3 MPC threshold requirement for any asset transfer with T+0 settlement on the Lux EVM.
- **Threshold custody and its proofs.** *Non-Custodial Securities Custody via Threshold Signing* [2] specifies the CGGMP21 (ECDSA) and FROST (Schnorr) protocols, the 2-of-3 wallet model, and the HSM attestation layer, and proves the non-custodial guarantee, liveness, and key-rotation safety.
- **Platform composition.** *Hanzo Platform Integration with Digital Securities* [3] shows how IAM, KMS, Gateway, and Base provide investor onboarding with KYC/AML, ATS trade execution, institutional MPC custody, and reporting for a regulated digital- securities stack.
- **Threshold-signing infrastructure.** *Hanzo Threshold Signing: MPC Key Management for AI Infrastructure* [4] documents the same FROST and CGGMP21 threshold protocols as a production (t, n) key-management system in which no party holds the complete key, corroborating the custody design.

4 Outcomes

1. **No single point of custody failure.** Because authorization requires a 2-of-3 threshold signature, neither the operator nor any single share-holder can move investor assets alone [1, 2].
2. **Regulatory role separation preserved.** The venue is designed to operate within Regulation ATS, broker-dealer, and transfer-agent frameworks while remaining non-custodial [1].
3. **Operational continuity.** Threshold shares can be rotated (reshared) without changing the on-chain address, supporting key hygiene and recovery without disrupting investor holdings [2].
4. **Defense in depth.** HSM attestation composes with the threshold protocol so that signing shares are hardware-attested without weakening the unforgeability guarantee [2].

References

- [1] Z. Kelling. *Non-Custodial Blockchain ATS: Architecture of a Regulatory-Compliant Securities Exchange*. Lux Partners. Source: `lux:lux-ats-architecture/lux-ats-architecture.tex`.
- [2] Z. Kelling. *Non-Custodial Securities Custody via Threshold Signing*. Lux Industries, Inc. Source: `lux:mpc-custody/mpc-custody.tex`.
- [3] Z. Kelling. *Hanzo Platform Integration with Digital Securities*. Hanzo Industries Inc. Source: `hanzo:hanzo-digital-securities-integration/hanzo-digital-securities-integration.tex`.
- [4] Z. Kelling. *Hanzo Threshold Signing: MPC Key Management for AI Infrastructure*. Hanzo Industries Inc. Source: `hanzo:hanzo-threshold-signing/hanzo-threshold-signing.tex`.