Post-Quantum Digital Securities at ACM: A Licensable, End-to-End Platform for Long-Lived Regulated Securities on a Quantum-Resistant Ledger

ACM Global Tech

Abstract

ACM Global Tech licenses and integrates an end-to-end, post-quantum regulated banking and digital-securities stack. This white paper describes ACM's Digital Securities Platform: issuance, custody, and transfer of tokenized securities on a regulated, quantum-resistant ledger whose cryptographic guarantees are designed to outlast the lifetime of the instruments they protect. The platform is built on the Lux Network's regulated post-quantum blockchain [1], deploys NIST-standardized post-quantum signatures as native EVM precompiles [2, 4], and realizes securities semantics through an ERC-1400 security-token standard hardened with post-quantum signature verification and threshold custody [3]. ACM Global Tech is a Web3 Alliance (W3A) member that licenses this intellectual property to partners who resell and co-build it for regulated institutions. We describe the platform's cryptographic foundation, its enforced-compliance securities semantics, and the intended outcomes for issuers, broker-dealers, and regulators.

1 The Problem: Securities Outlive Their Cryptography

A digital security is a long-lived obligation. A 30-year bond issued today must remain valid, transferable, and non-repudiable for three decades. The classical signature schemes that secure today's blockchains—ECDSA over secp256k1 and Ed25519—are vulnerable to a cryptographically relevant quantum computer, which would be able to forge signatures and recover private keys from public keys [2]. A "harvest now, decrypt later" adversary can record on-chain public keys and signed transactions today and forge against them once such hardware exists. For an instrument whose legal validity must persist for decades, the cryptographic root of trust must be quantum-resistant *at issuance*, not retrofitted after a break is announced.

Regulated digital securities add a second constraint. Beyond cryptographic durability, the platform must enforce transfer restrictions, identity and sanctions screening, and the role separation that securities law requires, without surrendering custody of investor assets to a single operator. A credible Digital Securities Platform must therefore satisfy *cryptographic longevity* and *regulatory enforceability* simultaneously.

2 ACM's Approach

ACM packages a licensable Digital Securities Platform that composes three proven layers from the underlying research stack into a single offering for issuers and partners.

Quantum-resistant ledger at genesis.

ACM builds on the Lux Network, a regulated post-quantum blockchain designed for the issuance,

custody, and transfer of digital securities, real-world assets, and compliant payments [1]. Post-quantum security is present from genesis rather than bolted on later [2].

Native post-quantum signatures.
The three NIST post-quantum algorithms—ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205)—are deployed as native EVM precompiles, reducing the cost of post-quantum verification from millions of gas in pure Solidity to the tens-of-thousands-of-gas range via an NTT-optimized lattice backend [4]. Migration is hybrid: a transaction may carry both a classical and a post-quantum signature and is accepted if either verifies, so the scheme remains secure as long as either assumption holds [2].

Securities semantics with enforced compliance.
Tokenized securities follow the Lux Security Token Standard, an ERC-1400 implementation on the post-quantum EVM that enforces transfer restrictions through on-chain compliance oracles linked to identity (I-Chain) DIDs, verifies post-quantum signatures, and uses MPC threshold signing for controller operations so that no single party can force a transfer [3].

ACM's role is commercial and integrative: as a W3A (w3a.foundation) member, ACM licenses this IP and partners to resell and co-build the stack for regulated institutions.

3 Cryptographic Foundation

The platform's technical guarantees trace directly to peer research in the Lux ecosystem:

- **Quantum threat model and hybrid migration.** *Post-Quantum Security for Digital Securities Infrastructure* [2] motivates the longevity requirement, deploys the three NIST algorithms as precompiles activated at genesis block 0, proves the hybrid classical/post-quantum scheme unforgeable as long as either underlying assumption holds, and reports gas benchmarks at NIST Levels 2, 3, and 5.
- **Precompile suite.** *Post-Quantum Cryptographic Suite for EVM: ML-KEM, ML-DSA, and SLH-DSA as Native Precompiles* [4] specifies the precompile interface, argues IND-CCA2 security preservation across the EVM boundary, and documents the gas-cost reduction relative to a Solidity implementation.
- **Security-token semantics.** *Lux Security Token Standard: ERC-1400 on Post-Quantum EVM with MPC Custody* [3] formally specifies token operations, proves the transfer-restriction mechanism sound and complete with respect to a compliance policy, and contrasts the design with ERC-3643 (T-REX), ERC-1404, and proprietary alternatives.
- **Platform thesis.** *The Lux Network: A Regulated, Post-Quantum Blockchain for Digital Securities, Real-World Assets, and Compliant Global Payments* [1] frames the regulated post-quantum ledger that the platform runs on.

4 Outcomes

The intended outcomes of the ACM Digital Securities Platform, as supported by the cited research, are:

1. **Cryptographic durability.** Securities are signed and verified under NIST post-quantum algorithms from issuance, so their validity is designed to survive the arrival of quantum adversaries [2, 4].

2. **Economic feasibility on-chain.** Native precompiles bring post-quantum verification into a practical gas range, making quantum-resistant securities economically viable on the EVM rather than prohibitively expensive [4].

3. **Enforced compliance without custody.** Transfer restrictions are enforced on-chain against identity DIDs, and controller actions require MPC threshold signing, so compliance is provable and no single party can unilaterally move investor assets [3].

4. **Non-disruptive migration.** The hybrid signature path lets existing classical workflows coexist with post-quantum verification during transition, accepting a transaction if either signature verifies [2].

References

[1] Z. Kelling. *The Lux Network: A Regulated, Post-Quantum Blockchain for Digital Securities, Real-World Assets, and Compliant Global Payments.* Lux Industries, Inc. Source: `lux:lux-whitepaper/lux-whitepaper.tex`.

[2] Z. Kelling. *Post-Quantum Security for Digital Securities Infrastructure.* Lux Industries, Inc. Source: `lux:post-quantum-securities/post-quantum-securities.tex`.

[3] Z. Kelling. *Lux Security Token Standard: ERC-1400 on Post-Quantum EVM with MPC Custody.* Lux Partners. Source: `lux:lux-security-token-standard/lux-security-token-standard.tex`.

[4] Z. Kelling. *Post-Quantum Cryptographic Suite for EVM: ML-KEM, ML-DSA, and SLH-DSA as Native Precompiles.* Lux Industries, Inc. Source: `lux:lux-pq-crypto-suite.tex`.