Post-Quantum Stablecoins: Regulated, Reserve-Attested Digital Cash on a Quantum-Resistant Ledger

ACM Global Tech

Abstract

A fiat-referenced stablecoin is a perpetual liability: a bearer claim on the issuer that may circulate, be redeemed, and re-enter circulation indefinitely, backed by reserves that are themselves long-dated. Yet every stablecoin in production today is authorized, transferred, and redeemed under classical signature schemes—ECDSA over secp256k1 and Ed25519—that a cryptographically relevant quantum computer would break [7]. A token minted under such a scheme is, in effect, a multi-decade obligation resting on a sub-decade cryptographic assumption, and a "harvest now, decrypt later" adversary can record the public keys and signatures securing the float today to forge against them later. At the same time, the 2025 U.S. stablecoin statute (the GENIUS Act) and the EU Markets in Crypto-Assets Regulation (MiCA) now require full reserve backing, redemption at par, and ongoing attestation [4, 5]. This paper describes ACM Global Tech's design for a regulated stablecoin in which issuance and redemption are signed with NIST ML-DSA (FIPS 204) on the Lux post-quantum ledger [2, 6, 7]; reserve keys are held under MPC threshold custody so no single operator can move them [9]; backing is proven continuously and operator-blind via threshold fully homomorphic encryption, with a regulator holding key shares able to compel lawful decryption [10, 11]; sanctions screening is enforced through privacy pools that prove non-association with illicit addresses without de-anonymizing every holder [12]; and every flow is screened in real time by ACM's AI/ML anti-money-laundering engine. ACM is a Web3 Alliance (W3A) member that licenses this intellectual property and partners to resell and co-build it for regulated institutions; the platform is assembled on Lux (blockchain, post-quantum cryptography, and FHE), Hanzo (AI and data infrastructure), and Zen (language models).

1 The Problem: A Perpetual Liability on a Perishable Assumption

A stablecoin is not a payment message that lives for a few seconds and then ceases to matter. It is a standing liability of its issuer—a tokenized, bearer-transferable claim to one unit of fiat, redeemable on demand and backed by reserves held against the entire outstanding float. The reserves behind a well-run stablecoin are deliberately long-dated and conservative: short-term government securities, reverse repo, and insured cash. The instrument is, structurally, perpetual: there is no maturity date at which the obligation extinguishes itself. As long as a unit circulates, the issuer owes redemption.

This creates a temporal mismatch that the industry has not confronted. The cryptography that authorizes minting, governs custody of the reserve keys, and validates redemption is classical: ECDSA over the secp256k1 curve and Ed25519. Both rest on the hardness of the elliptic-curve discrete logarithm problem, which Shor's algorithm solves in polynomial time on a sufficiently large quantum computer [7]. A cryptographically relevant quantum computer would let an adversary recover private keys from the public keys that necessarily appear on-chain, forge issuer

authorizations, and drain or counterfeit the float. The threat does not wait for that hardware to exist. Under a "harvest now, decrypt later" posture, an adversary records the public keys and signed transactions that secure today's stablecoins and forges against them the moment a capable machine arrives [7]. A token minted today is therefore a multi-decade obligation whose integrity rests on an assumption that is not expected to survive the same horizon. The mismatch is not hypothetical risk management; it is a maturity transformation in the cryptographic domain, and it is mispriced at zero.

The regulatory frame has moved in parallel, and it sharpens the problem rather than relaxing it. The U.S. GENIUS Act establishes a federal regime for payment stablecoins that requires issuers to hold reserves backing the outstanding supply on at least a one-to-one basis in high-quality liquid assets, to honor redemption at par, and to disclose reserve composition under recurring examination [4]. In the European Union, MiCA classifies a fiat-pegged token as an e-money token (EMT), obliges the issuer to back it with fully segregated reserves, and grants holders a legal right of redemption at par at any time [5]. Both regimes presume the issuer can *prove*, on a continuing basis, that the reserves exist and are sufficient—and both presume the authorization chain that mints and burns the token is sound. A stablecoin that satisfies the reserve and redemption rules but signs them with breakable cryptography satisfies the letter of the rule while undermining the asset it is meant to protect. A credible design must therefore meet two constraints at once: *cryptographic longevity* commensurate with a perpetual liability, and *regulatory provability* of backing, redemption, and clean flows.

2 ACM's Approach

ACM packages a licensable regulated-stablecoin platform that composes proven layers of the underlying research stack into a single offering for issuers and partners. The design treats post-quantum authorization, custody, screening, and proof-of-reserves as first-class properties of the instrument rather than operational add-ons.

Post-quantum authorization at the mint and the redemption.
Issuance (mint) and redemption (burn) are authorized by signatures under ML-DSA, the NIST module-lattice digital signature standard of FIPS 204 [2], verified natively on the Lux post-quantum ledger. ML-DSA is deployed alongside the companion NIST standards ML-KEM (FIPS 203) for key establishment and SLH-DSA (FIPS 205) as a hash-based signature fallback, all exposed as native EVM precompiles so that post-quantum verification costs are practical on chain rather than prohibitive [1, 3, 8]. Because the authorization on the most consequential operations—creating and destroying the liability—is quantum-resistant from genesis, the token's integrity is designed to outlast the instrument it secures [7, 6].

Hybrid migration, not a flag day.
Transition is hybrid: a transaction may carry both a classical and a post-quantum signature and is accepted if either verifies, so the authorization path remains secure as long as *either* assumption holds, and existing classical tooling continues to function during the migration [7]. There is no moment at which the system is simultaneously off the old scheme and not yet on the new one.

MPC threshold custody of reserve keys.
The keys that authorize minting and that control the on-chain representation of reserves are never held by a single operator. They are generated and used under multi-party computation

threshold signing, so that a quorum—rather than any one party—is required to authorize an operation [9]. No single insider, and no single compromised host, can mint supply or move reserves unilaterally.

Real-time AI/ML AML on every flow.
ACM operates an AI/ML anti-money-laundering engine that scores each issuance, transfer, and redemption in real time, rather than relying on after-the-fact batch review. The engine is built on Hanzo AI and data infrastructure and Zen language models, and it composes with the on-chain sanctions controls described in Section 4.

T+0 redemption.
Because the authorization, the reserve representation, and the screening are all on the same ledger, redemption at par is designed to settle same-day (T+0): the burn of the token and the release of the corresponding reserve claim are a single atomic, post-quantum-authorized operation rather than a multi-day reconciliation between disjoint systems.

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. ACM additionally ships a Stripe-class payment service provider (PSP) and full Banking-as-a-Service, so that an issuer or partner can plug fiat on- and off-ramps, card acceptance, and account infrastructure into the same regulated rail rather than integrating a separate processor.

3 Reserve Attestation: Continuous, Operator-Blind Proof of Backing

The weakest link in today's stablecoin assurance model is the attestation letter. An accounting firm samples the reserve at a point in time, signs a report, and the market trusts that the composition has not materially changed until the next report. Between reports the holder has no cryptographic basis for believing the backing is intact; the GENIUS Act and MiCA both push toward more frequent disclosure, but periodic disclosure is still periodic [4, 5]. The structural problem is that the proof is a human assertion about a private ledger, refreshed monthly, not a property of the system that holds continuously.

ACM's design replaces the periodic letter with a continuous, operator-blind cryptographic proof of full backing. The reserve ledger—the record of cash and high-quality liquid assets held against the outstanding float—is maintained under threshold fully homomorphic encryption (threshold FHE) [10]. Balances and positions are encrypted; the aggregate sufficiency condition (total reserves $\geq$ total outstanding supply) is evaluated homomorphically over the encrypted state, so the system can publish a continuously updated proof that the backing constraint holds *without* any party decrypting the underlying positions. The proof is operator-blind: ACM, the issuer, and any individual custodian see that the constraint is satisfied but do not, through this channel, learn the line-item composition of a counterparty's holdings.

Lawful inspection is built in rather than bolted on. The FHE decryption key is split into n shares under a t-of-n threshold scheme, and a regulator (or a panel of regulators) holds a quorum of those shares [11]. When a supervisory authority is entitled to inspect the underlying reserve detail, its quorum of shares compels decryption of the relevant encrypted state; no cooperation from the operator is required, and the operator cannot prevent it. The result is a proof-of-reserves that is *continuous* (the sufficiency predicate holds at every block, not once a month), *operator-blind* (no party must be trusted to refrain from peeking at others' positions to produce the proof),

and *lawfully transparent* (a regulator with the requisite key shares can always force disclosure for inspection). This is the attestation letter inverted: instead of trusting a periodic human assertion about a private ledger, the market relies on a standing cryptographic predicate, and the regulator holds the key that opens it.

4 Compliance Mapping

The design maps directly onto the two regimes that now govern fiat-pegged tokens. The mapping is intended as a faithful description of how the architecture addresses each obligation, not as legal advice; the controlling text in each jurisdiction governs.

GENIUS Act (United States). The statute conditions a payment stablecoin on full reserve backing in high-quality liquid assets, par redemption, and recurring disclosure under examination [4]. The platform addresses these as follows. *Full backing* is enforced as the continuously evaluated sufficiency predicate of Section 3, so backing is a standing cryptographic property rather than a monthly assertion. *Par redemption* is realized as the T+0 atomic burn-and-release operation, post-quantum authorized, so the holder's redemption right is executed on-ledger rather than queued behind off-chain reconciliation. *Examination and disclosure* are served by the regulator-held threshold-FHE key shares, which let a supervisor inspect reserve detail on demand without operator cooperation. *Custody integrity*—the concern that an issuer could divert reserves—is constrained by MPC threshold custody, under which no single operator can move reserve-controlling keys [9].

MiCA e-money tokens (European Union). MiCA treats a fiat-pegged token as an e-money token, requiring fully segregated reserves and a legal right of redemption at par at any time [5]. *Segregation and sufficiency* are expressed by the operator-blind reserve ledger and its homomorphic sufficiency proof; *redemption at par at any time* is the same T+0 atomic operation, available continuously because authorization, reserve representation, and screening share one ledger. The result is that the EMT holder's statutory redemption right is enforced by the mechanics of the instrument rather than by the issuer's operational diligence.

Sanctions screening via privacy pools. Both regimes, and the broader AML/CFT framework, require that issuers prevent sanctioned and illicit actors from using the rail—without that obligation collapsing into surveillance of every lawful holder. The platform enforces this with privacy pools: a holder proves, in zero knowledge, that their funds are *not* associated with a published set of illicit or sanctioned addresses, and may transact on the strength of that proof without revealing their identity or full transaction graph to the public [12]. Non-association is proven rather than identity disclosed: the compliant majority transacts with privacy, while the illicit minority is provably excluded. This on-chain control composes with ACM's real-time AI/ML AML engine, which scores flows against behavioral and network-level risk signals; the privacy pool establishes a cryptographic exclusion of known-bad addresses, and the AML engine adds dynamic, model-driven screening on top.

5 Outcomes

The following are framed as design goals and targets supported by the cited research, not as realized client metrics; no client names or performance figures are asserted.

1. **Cryptographic durability commensurate with a perpetual liability.** Minting and redemption are authorized under NIST ML-DSA from genesis, with ML-KEM and SLH-DSA available as companion primitives, so the integrity of the float is designed to survive the arrival of quantum adversaries rather than to be retrofitted after a break [2, 1, 3, 7].

2. **Continuous, provable backing.** Full reserve backing is a standing cryptographic predicate evaluated operator-blind over an encrypted reserve ledger, replacing the periodic attestation letter with continuous proof and lawful, key-share-gated regulator inspection [10, 11].

3. **No single point of custody.** Reserve and minting keys are held under MPC threshold signing, so no single operator can mint supply or move reserves unilaterally [9].

4. **Compliant privacy.** Sanctions screening is enforced by proof of non-association via privacy pools and by real-time AI/ML AML scoring, so the rail excludes illicit actors without deanonymizing every lawful holder [12].

5. **Same-day redemption.** Redemption at par is designed to settle T+0 as a single atomic, post-quantum-authorized operation, satisfying the redemption rights that both the GENIUS Act and MiCA require [4, 5].

References

[1] National Institute of Standards and Technology. *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)*. U.S. Department of Commerce, 2024.

[2] National Institute of Standards and Technology. *FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA)*. U.S. Department of Commerce, 2024.

[3] National Institute of Standards and Technology. *FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA)*. U.S. Department of Commerce, 2024.

[4] United States Congress. *Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act)*—federal framework for the issuance and reserve backing of payment stablecoins, 2025.

[5] European Union. *Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA)*, Official Journal of the European Union, 2023. See in particular the Title IV provisions on e-money tokens.

[6] 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`.

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

[8] 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`.

[9] Z. Kelling. *MPC Threshold Custody for Regulated Digital Assets*. Lux Partners. Source: `lux:mpc-custody/mpc-custody.tex`.

[10] Z. Kelling. *Threshold Fully Homomorphic Encryption on the Lux Network*. Lux Industries, Inc. Source: `lux:lux-tfhe/lux-tfhe.tex`.

[11] Z. Kelling. *Threshold FHE for Compliance: Operator-Blind Computation with Regulator-Gated Decryption*. Lux Partners. Source: `lux:threshold-fhe-compliance/threshold-fhe-compliance.tex`.

[12] Z. Kelling. *Lux Privacy Pool: Proof of Non-Association for Compliant Confidential Transfers*. Lux Partners. Source: `lux:lux-privacy-pool/lux-privacy-pool.tex`.