--- ---

ETERNAX LABS RESEARCH REPORT · JULY 2026

Your Chain Will Not Save You: Post-Quantum Institutional Risk Across Ethereum, Solana, and Canton

Chain upgrades will not automatically protect institutional tokenization, stablecoins, custody, DeFi liquidity, or private settlement. Ethereum, Solana, and Canton carry non-upgradeable cryptographic dependencies across immutable contracts, frozen standards, exposed public keys, identity systems, and historical encrypted data. EO 14412 now makes post-quantum cryptographic inventory and migration a federal compliance priority. For new issuance, the strategic answer is not retrofit. It is PQ-native rails.

$71T+
Tokenization, DeFi TVL, stablecoins, and settlement rails.

$9T/mo
Canton settlements. Zero PQ algorithms deployed.

700+
Institutions and market participants mapped.

0
Chains with a concrete PQ migration timeline.

AUTHORS

PAARRTHHH BIRLA, DR. CHEN FENG, DARIIA PORECHNA · ETERNAX LABS

PUBLISHED

JULY 1, 2026

AUDIENCE

BOARDS, RISK COMMITTEES, TOKENIZATION TEAMS, STABLECOIN ISSUERS, CUSTODIANS, DEFI OPERATORS

REPORT INDEX

15-minute read | 3 chains | 700+ institutions and market participants mapped | 4-point action framework | 44 FAQs | July 1, 2026

ANSWER IN BRIEF

Ethereum, Solana, and Canton cannot be made fully post-quantum safe through chain upgrades alone. Institutional exposure sits in immutable contracts, frozen token standards, exposed public keys, identity systems, custody workflows, and historical encrypted settlement data.

The institutional decision is therefore not only whether a chain may upgrade later. It is whether the product, compliance gate, custody stack, liquidity path, and settlement record can survive the parts that do not migrate. New issuance should evaluate PQ-native rails before avoidable migration debt becomes permanent.

WHAT QUANTUM EXPOSURE LOOKS LIKE

A forged ONCHAINID claim can bypass compliance gates on regulated tokenized securities. $32 billion in ERC-3643 assets can move to unauthorized wallets while the issuer's legal control layer appears valid onchain. A forged ERC-2612 permit can drain stablecoin balances routed through DeFi approval infrastructure without the owner transacting. A compromised Solana

> authority key can mint, freeze, or seize tokenized assets. A harvested Canton encrypted view can expose private institutional settlement history once a cryptographically relevant quantum computer arrives. This is not abstract blockchain security. It is tokenization, DeFi liquidity, custody control, stablecoin authorization, and settlement privacy exposure across the rails institutions already use.

> ***The Wake-Up Call:*** *Every major chain can publish a post-quantum roadmap. That does not save your product. A protocol upgrade can change the chain layer, but it cannot rewrite immutable contracts, frozen token standards, hardcoded permit interfaces, ONCHAINID compliance logic, SPL Token authority models, custody integrations, or historical encrypted settlement data. PQ migration is not a chain upgrade. It is a product, compliance, custody, and market-structure migration. The conservative institutional path is not to wait for legacy chains to complete multi-year transitions. It is to issue on PQ-native infrastructure, like EternaX, where migration debt does not accumulate.*

> "Quantum computers will break currently deployed public-key cryptography, and significantly weaken symmetric key cryptography."
>
> MICHELE MOSCA, INSTITUTE FOR QUANTUM COMPUTING | CYBERSECURITY IN AN ERA WITH QUANTUM COMPUTERS

Executive Summary

Institutional digital assets totaling $38B+ in Ethereum DeFi TVL, $32B+ in regulated tokenized securities, $80B+ in stablecoin market cap with native permit exposure, $6-8B in Solana DeFi TVL, and $9 trillion per month in Canton settlement volume run on Ethereum, Solana, and Canton Network. All three chains rely on elliptic curve cryptography that Shor's algorithm will break. The market's default assumption is that chains will upgrade and institutions can wait. This report demonstrates why that assumption is dangerous.

The issue is not only transaction signing. Across all three chains, critical cryptographic dependencies are hardcoded into standards, compiled into validator binaries, embedded in immutable contracts, frozen into interfaces, bound into identity systems, or preserved forever in historical encrypted data. Chain upgrades can change future protocol behavior. They do not automatically repair the products, compliance gates, custody workflows, liquidity integrations, or settlement records already built on top.

> *Five of eight institutional ERC standards deploy on a PQ-native chain with zero modification. Two regulated-asset standards need scoped module upgrades. One standard must be replaced entirely. On Solana and Canton, quantum vulnerability extends from address derivation through consensus with no deployed PQ defense at any layer.*

This report focuses on the institutional markets sitting directly on these rails: tokenized securities, tokenized funds, stablecoins, DeFi liquidity, custody platforms, fund administration, wallet infrastructure, and post-trade settlement.

KEY FINDINGS

Ethereum: Five layers of non-upgradeable ECDSA. ERC-3643 compliance layer ($32B+ tokenized) uses quantum-vulnerable claim verification. ERC-2612 permit ($80B+ in token market cap with native permit, $38B+ DeFi TVL routing through permit infrastructure) is hardcoded with ECDSA-specific parameters. Immutable contracts ($15B+ TVL: Uniswap Permit2/V2/V3, Compound V2, WETH9) are permanent.

Solana: Ed25519 across every authority key, every account, every validator. Addresses are raw public keys with zero address-level quantum protection. $6-8B DeFi TVL exposed. SPL Token is permanently immutable. GPU verification pipeline is hardcoded for Ed25519. Solana Foundation / Project Eleven testnet showed ~90% throughput decline under PQ. Falcon roadmap exists but no mainnet deployment, no timeline, no hardware wallet support.

Canton: $9 trillion/month in settlements ($60T+ cumulative) on quantum-vulnerable Ed25519/ECDSA P-256. Namespace identity permanently bound to classical root key fingerprint. Synchronizer enforces minimum scheme set, making partial migration technically impossible. Zero PQ algorithms deployed, zero public PQ documentation. Every encrypted transaction view is vulnerable to harvest-now-decrypt-later.

Conclusion: Chain migration is only the beginning. Existing products, compliance layers, immutable contracts, custody integrations, and historical settlement data still need their own migration plan. For new issuance, PQ-native infrastructure like EternaX, built on SPHINCS+/SLH-DSA (NIST FIPS 205) from genesis, is the only path that eliminates migration debt entirely.

Board-Level Translation: From Cryptographic Risk to Business Risk

For executives, the post-quantum question is not whether an algorithm is elegant. It is whether a tokenized product can remain transferable, compliant, private, liquid, and insurable when its cryptographic assumptions expire.

EXPOSURE	TECHNICAL ISSUE	BUSINESS CONSEQUENCE
Ethereum tokenized funds	ECDSA accounts, ecrecover, permit flows, immutable DeFi contracts	Admin-key exposure, forged approvals, liquidity migration debt, unresolved custody diligence
ERC-3643 securities	ONCHAINID claim verification depends on ECDSA	Forged compliance attestations, transfer-rule failure, regulatory control breakdown
Solana stablecoins and RWAs	Ed25519 account authority, SPL Token immutability, hardcoded verification path	Issuer authority exposure, freeze/mint-control risk, ecosystem-wide migration burden
Canton settlement	ECIES P-256 encrypted views, namespace key binding, Synchronizer scheme gate	Historical privacy loss, identity migration shock, simultaneous-participant coordination risk
Custody and MPC stacks	Final onchain signature remains ECDSA or Ed25519	MPC reduces operational key risk but does not remove algorithm-level quantum exposure

WHY ETERNAX EXISTS

EternaX exists because post-quantum migration is not only an algorithm swap. It is a market-infrastructure redesign. Institutional rails need PQ-safe accounts, signatures, verifier logic, identity, custody workflows, compliance modules, and settlement assumptions from genesis.

That is the core architectural difference: EternaX does not ask institutions to wait for legacy chains to repair cryptographic debt after liquidity, custody, and compliance integrations become immovable. It removes the debt before issuance.

SOURCE-GRADE FOUNDATION

The cryptographic claims in this report are anchored to primary standards and protocol documentation: NIST's finalized PQC standards, FIPS 205 / SLH-DSA, NSA CNSA 2.0, ERC-2612, Solana runtime and precompile documentation, and Canton security and key-management documentation. Institution-specific exposure and dollar figures should be refreshed against live product disclosures before each publication cycle.

> "The key is to be on this journey today and not wait until the last minute."
>
> ROB JOYCE, FORMER DIRECTOR OF NSA CYBERSECURITY | CISA, NIST, AND NSA QUANTUM-READINESS GUIDANCE

Cross-Chain Post-Quantum Exposure Summary

	Ethereum	Solana	Canton
Address Derivation	secp256k1. No fix.	Ed25519. No fix.	Ed25519/P-256. ECC only.
Transaction Signing	ECDSA. Hard fork req.	Ed25519. All auth keys.	Ed25519/ECDSA. Zero PQ.
Precompiles / Runtime	ecrecover. No fix.	Ed25519Verify. Native.	Pluggable API. Path exists.
Immutable Contracts	Permit2/V2/V3. Permanent.	SPL Token. BPFLoader2.	Daml abstracted. Clean.
Standard-Level ECDSA	ERC-2612 v/r/s. Hardcoded.	N/A (no ERC equiv)	No hardcoded ECDSA.
Consensus Layer	PoS. Upgradeable.	BLS aggregation. No PQ.	Scheme gate. All or none.
Privacy / HNDL Risk	Public chain. N/A.	Public chain. N/A.	ECIES P-256. HNDL risk.
	5 of 7 critical	5 of 7 critical	4 of 7 critical

Non-upgradeable or no fix · Upgrade path exists, not deployed · Clean or abstracted · Not applicable or upgradeable

Red: non-upgradeable or no fix available. Amber: upgrade path exists but not deployed. Green: clean or abstracted. Grey: not applicable.

THE WAKE-UP CALL

Chain Upgrades Do Not Fix Your Product

Every major chain now has, or will claim to have, a post-quantum roadmap. That is not enough. The institutional exposure does not end at the protocol layer. It lives inside products, standards, custody flows, compliance gates, immutable contracts, frozen interfaces, and historical settlement data.

A chain upgrade can change the base layer. It cannot rewrite your issued token, your permit interface, your ONCHAINID compliance logic, your SPL Token authority model, your custody integration, or the encrypted settlement history already recorded on quantum-vulnerable keys. This is the blind spot this report is designed to expose.

What a Chain Upgrade Does NOT Fix

EVEN AFTER ETHEREUM HARD FORKS TO PQ

ERC-3643 ONCHAINID still uses ECDSA ecrecover. Your $32B in regulated securities still has forgeable compliance gates.

ERC-2612 permit still requires (v, r, s). $80B+ in tokens cannot accept PQ signatures through their existing ABI.

Permit2, V2/V3, Compound V2, WETH9 are still immutable. $15B+ TVL in contracts with permanent ECDSA logic.

EVEN AFTER SOLANA MIGRATES VALIDATORS TO PQ

SPL Token is still immutable via BPFLoader2. The entire $6-8B token ecosystem must migrate to a new program.

Throughput drops ~90%. Confirmed by Solana Foundation / Project Eleven testnet (April 2026). GPU pipeline requires full CUDA rewrite.

Every address is a raw public key. Zero address-level quantum protection. All accounts permanently exposed from creation.

EternaX eliminates all three problems: SPHINCS+ signing from genesis, ~2% TPS loss (not ~90%), and PQ-safe address derivation with no exposed classical keys.

EVEN AFTER CANTON DEPLOYS ML-DSA

Namespace identity must be destroyed and recreated. Canton's own documentation states root signing keys cannot be rotated without losing the namespace.

$60T+ in historical settlements is still decryptable. Every prior trade between Goldman Sachs, DTCC, JPMorgan, HSBC can be decrypted.

Throughput drops ~88%. $9T/month in settlements faces systemic risk during migration. AWS/GCP KMS do not support PQ signing.

700+ institutions must coordinate simultaneously. Synchronizer enforces minimum scheme set. Partial migration is technically impossible.

EternaX eliminates all four problems: PQ identity from genesis, ~2% TPS loss, no coordination required, and PQ encryption protecting settlement privacy from day one.

> *The problem is not the chain. The problem is the application layer. Your products, your standards, your compliance infrastructure, your immutable contracts, your custody integrations. Chain upgrades do not fix your products. You cannot outsource PQ risk to protocol teams. With verified PQC standards, federal inventory requirements, and the regulatory cascade reaching custodians, vendors, and contractors, the window for institutional passivity is closing. The question is not "when will the chain upgrade?" The question is "when will you move your products to rails that do not require repair?"*

MIGRATION CHALLENGE	ETHEREUM	SOLANA	CANTON	PQ-NATIVE CHAIN
Address / identity model	Requires new account model; public keys exposed after first tx	Requires new account model; addresses ARE raw public keys (always exposed, zero address-level protection)	Namespace = hash of root key fingerprint. Changing key type destroys identity. Canton docs: "cannot be rotated without losing the namespace"	Solved at genesis
Transaction signing	Coordinated hard fork, all clients	Coordinated upgrade, all validators; GPU sigverify pipeline hardcoded for Ed25519 CUDA requires full rewrite	Six-layer signing across topology, confirmations, mediator, transfers, ACS commitments, sequencer auth	Solved at genesis
Signature precompiles	ecrecover cannot be patched	Ed25519Verify is native code; programs using precompiles inherit vulnerability after migration	Pluggable API (application-layer advantage); protocol layer still requires full migration	PQ verifier from day one
Immutable contracts	Permit2, V2/V3, WETH9: permanent	SPL Token: BPFLoader2, permanent	No immutable contracts (application-layer advantage)	No legacy to inherit
Broken standards	ERC-2612: must be replaced; ERC-3643: ONCHAINID must be rebuilt	SPL Token: immutable, all authority keys (mint, freeze, upgrade) are Ed25519-locked. Token-2022 Confidential Transfers derive ElGamal keys from Ed25519. Transaction ID is first Ed25519 signature.	N/A (Daml abstraction, application-layer advantage)	PQ-permit + PQ-ONCHAINID from day one

MIGRATION CHALLENGE	ETHEREUM	SOLANA	CANTON	PQ-NATIVE CHAIN
Consensus	PoS: consensus-layer PQ key registry proposed (EIP-8141, Hegotá H2 2026). leanXMSS + SNARK aggregation.	Alpenglow BLS aggregation: no PQ equivalent exists. Research active (LaBRADOR, Raccoon) but not production-ready.	Synchronizer enforces minimum scheme set; partial migration technically impossible	PQ-safe consensus from day one
Privacy / HNDL	Public chain: N/A	Public chain: N/A	ECIES P-256: $60T+ historical views exposed. Cannot be un-collected.	PQ encryption from day one
Infrastructure dependencies	L2s, wallets, custody, DeFi integrations	Wallets, custody, hardware (no Falcon HSM support); vault fee payers still Ed25519	AWS/GCP KMS do not support PQ signing; production deployments blocked until cloud providers add support	No legacy dependencies
Performance under PQ	~84% TPS loss (modeled, SPHINCS+ substitution)	~90% TPS loss (Solana Foundation / Project Eleven testnet, April 2026)	~88% TPS loss (modeled, SPHINCS+ substitution)	~2% TPS loss
Estimated migration timeline	L1 target ~2029; full execution-layer migration years beyond (pq.ethereum.org). EIP-8141 proposed for Hegotá H2 2026.	Falcon prototypes on GitHub, no mainnet deployment, no timeline set. FIPS 206 (Falcon) not yet finalized.	Unknown. Zero public documentation, zero roadmap published as of June 2026.	Day one

Historical precedent: SHA-1 to SHA-2 took over a decade. 3DES to AES took 5-20 years. PQ migration is orders of magnitude more complex, touching every layer simultaneously. No blockchain has completed one. Ethereum targets L1 upgrades by ~2029 with full execution-layer migration taking additional years (pq.ethereum.org). Solana has prototypes but no mainnet deployment or timeline. Canton has zero public roadmap. Academic research estimates 5-7 years optimistic, 10-15 years realistic for full blockchain PQ migration (JBBA, 2026). EternaX eliminates this migration timeline entirely: institutions deploy on PQ-native rails from day one rather than waiting for legacy chains to complete multi-year transitions.

THE REGULATORY CLOCK

The Federal PQC Clock: Verified Sources, Not Roadmap Comfort

The United States has moved from guidance to enforcement. Finalized NIST standards, binding inventory requirements, and Executive Order 14412 create a compliance cascade that reaches every institutional digital-asset product through procurement, custody, and settlement.

> "We encourage system administrators to start integrating them into their systems immediately, because full integration will take time."
>
> DUSTIN MOODY, NIST PQC PROJECT LEAD | NIST FINALIZED PQC STANDARDS ANNOUNCEMENT

VERIFIED SOURCE	WHAT IT ESTABLISHES	INSTITUTIONAL IMPLICATION
NSM-10 White House, May 2022	Quantum-vulnerable cryptography classified as national security risk. Migration planning directed.	PQC is a national-security transition program, not optional research.
OMB M-23-02 November 2022	Federal agencies directed to inventory and prioritize migration of quantum-vulnerable cryptography.	CBOM-style diligence becomes the institutional baseline.
NSA CNSA 2.0 September 2022	Quantum-resistant algorithm requirements for National Security Systems. Preference dates 2025-2026, required dates 2030-2033.	Financial market infrastructure will face the same assurance expectations.
NIST FIPS 203, 204, 205 August 2024	ML-KEM, ML-DSA, and SLH-DSA (SPHINCS+) finalized as federal standards.	Institutions now have recognized standards against which vendors and settlement rails can be evaluated.
NIST IR 8547 November 2024	ECDSA/RSA deprecated after 2030 (112-bit security). All ECDSA/RSA/EdDSA disallowed after 2035.	Every chain using ECDSA or Ed25519 is on a published deprecation/disallowance schedule.
Executive Order 14412 "Securing the Nation Against Advanced Cryptographic Attacks" White House, June 22, 2026	First enforceable federal PQC deadlines. 30 days: agency PQC leads. 90 days: OMB binding guidance. 180 days: FAR contractor compliance rule (deadline Dec 31, 2030). 270 days: CISA/NIST CBOM guidance. Dec 31, 2031: PQC for all federal digital signatures.	Converts PQC from research into procurement gates. CBOM will expose ECDSA/EdDSA dependencies across custody, tokenization, and settlement. The order states adversaries "may already be collecting" encrypted data for future quantum decryption.

Executive Order 14412: The Compliance Cascade into Digital Assets

EO 14412 (Federal Register Vol. 91, No. 121, June 25, 2026) directly binds federal agencies. Its private-sector impact flows through procurement, federal contractors, critical-infrastructure expectations, regulated-client diligence, vendor risk reviews, and CBOM disclosure. That distinction matters: the order does not instantly regulate every crypto institution, but it creates the compliance standard those institutions will increasingly be measured against.

Channel 1: FAR Procurement (Section 6c). Federal contractors must comply with NIST FIPS PQC by December 31, 2030. Digital-asset vendors with federal contract exposure, federal clients, or federal-adjacent market infrastructure relationships will be pulled into that requirement first.

Channel 2: CBOM Disclosure (Section 5d). By ~March 2027, CISA and NIST publish CBOM guidance: machine-readable inventories of every algorithm, key, and protocol. For a blockchain product, that means declaring ECDSA, Ed25519, ECIES, permit logic, identity-verification logic, and custody signing dependencies as deployed cryptographic components. A roadmap is not a CBOM entry.

Channel 3: Critical Infrastructure Pressure (Section 5a). Financial market infrastructure, clearing, settlement, custody, and post-trade technology providers will face higher assurance expectations even where the order reaches them indirectly through clients, supervisors, procurement, and resilience standards.

Channel 4: Regulated Client Cascade. BlackRock, Goldman Sachs, JPMorgan, State Street, and other regulated financial institutions will increasingly ask their digital-asset vendors the same question: which

deployed algorithms secure this product today, and are they aligned with NIST-approved PQC migration plans?

Channel 5: Section 6(d) Vulnerability Disclosure. Contractor vulnerability disclosure expands to cover the use of non-FIPS approved algorithms. For products touching federal procurement or federal-adjacent systems, ECDSA and Ed25519 dependencies become diligence items, not abstract cryptography.

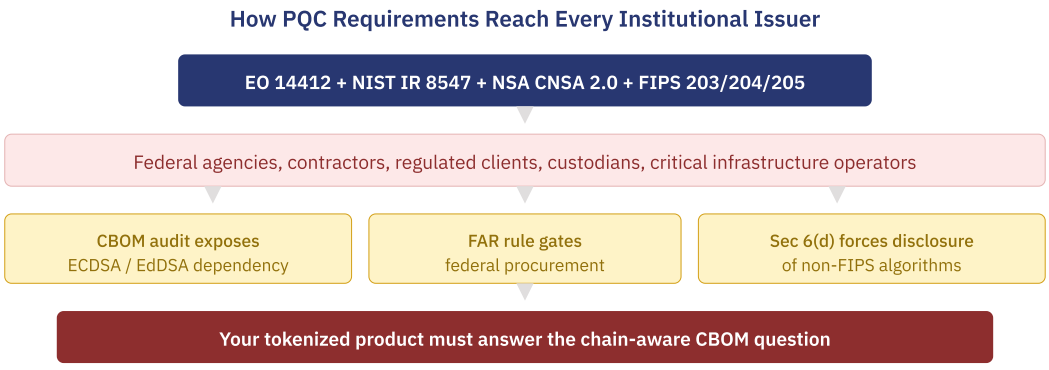
What a CBOM Audit Returns Today

A CBOM audit reports what is deployed, not what is planned:

CHAIN	TX SIGNING ALGORITHM	NIST PQ STATUS	PQ TPS IMPACT	IN-PLACE MIGRATION PATH	CBOM RESULT
Ethereum	ECDSA (secp256k1)	Deprecated 2030 / Disallowed 2035	~84% loss	Requires hard fork + account migration + immutable contract ecosystem	**FAIL**
Solana	EdDSA (Ed25519)	Disallowed 2035	~90% loss	Requires runtime overhaul + GPU pipeline rewrite + SPL Token migration	**FAIL**
Canton	Ed25519 / ECDSA P-256	Disallowed 2035	~88% loss	Namespace identity impossibility + Synchronizer gate + KMS blocker	**FAIL**
Stellar	EdDSA (Ed25519)	Disallowed 2035	~90% loss	Requires protocol upgrade across validator network	**FAIL**
Bitcoin	ECDSA (secp256k1)	Deprecated 2030 / Disallowed 2035	No PQ proposal	No consensus on PQ migration path	**FAIL**
EternaX	SPHINCS+ / SLH-DSA (FIPS 205)	NIST Approved	~2% loss	Native from day one. No migration required.	**PASS**

VERIFIED SOURCES

White House: Executive Order 14412. Federal Register: Vol. 91, No. 121, FR Doc 2026-12909. NIST: IR 8547. See also: Cloudflare analysis, Jenner & Block analysis.



> *The regulatory clock is not waiting for multi-year blockchain governance debates. EO 14412 creates named federal owners, hard dates, and procurement consequences. Its pressure reaches private digital-asset infrastructure through contractors, regulated clients, vendor diligence, and CBOM disclosure. CBOM guidance (due ~March 2027) will force machine-readable disclosure of every deployed algorithm. What is deployed today is what gets reported. A chain roadmap is not a CBOM entry. EternaX, built on SPHINCS+/SLH-DSA (NIST FIPS 205), is designed to return a PASS on the chain-aware CBOM question from day one.*

CHAIN 1 OF 3

Ethereum and the EVM Ecosystem

Ethereum has five layers where ECDSA (secp256k1) is embedded in ways no software upgrade can remove. Each layer is independently non-upgradeable. Together they constitute a permanent architectural commitment to quantum-vulnerable cryptography.

Five Layers of Non-Upgradeable ECDSA in Ethereum

LAYER 1 **Address Derivation**	Every Ethereum address is derived from a quantum-vulnerable key. Once you send a transaction, your public key is exposed permanently. Every address that has ever transacted is compromisable.
LAYER 2 **Transaction Signing**	Every transaction is validated using quantum-vulnerable ECDSA. Compiled into all 5 node clients. EIP-8141 (Hegotá H2 2026) proposes account abstraction for signature agility. Full migration years beyond.
LAYER 3 **ecrecover Precompile**	The built-in signature checker (ecrecover) is hard-wired into the blockchain software. Not a smart contract. Cannot be upgraded by governance. Used by every permit, every identity claim, every multisig.
LAYER 4 **Immutable Contracts**	Uniswap Permit2, V2/V3 Pools, Compound V2, Curve base pools, Balancer V2 Vault, WETH9, ENS Registry. No proxy. No upgrade function. No admin key. ECDSA logic is permanent for the lifetime of the chain.
LAYER 5 **Frozen Interfaces**	USDC, DAI, PYUSD, stETH, cbETH permit ABI: (uint8 v, bytes32 r, bytes32 s). SPHINCS+ signatures (7.8KB+) cannot fit. Changing the ABI breaks Uniswap, 1inch, 0x, Fireblocks, Anchorage, and every caller.

NONE OF THESE FIVE LAYERS CAN BE FIXED ON EXISTING CHAINS. ALL FIVE ARE SOLVED AT GENESIS ON A PQ-NATIVE CHAIN.

Broken Standards: ERC-3643, ERC-2612, ERC-1400

Three of the eight most institutionally relevant ERC standards have ECDSA embedded at levels that prevent clean post-quantum migration. They are ordered here by institutional exposure severity.

STANDARD	INSTITUTIONAL FUNCTION	ECDSA LOCATION	SEVERITY	WHAT BREAKS UNDER QUANTUM ATTACK
ERC-3643	Regulated security tokens. $32B+ tokenized across 180+ jurisdictions. DTCC/SEC endorsed.	Embedded in ONCHAINID claim verification. isClaimValid verifies claim issuer signatures via ECDSA ecrecover.	CRITICAL	Attacker fabricates KYC/AML attestations, bypasses all compliance gates, moves regulated securities to ineligible wallets.
ERC-2612	Gasless approvals. USDC, DAI, PYUSD, institutional DeFi flows.	Hardcoded in spec. permit(... uint8 v, bytes32 r, bytes32 s). Uses ecrecover. v/r/s is ECDSA-specific.	CRITICAL	Attacker drains any token balance by forging gasless approvals. No onchain transaction by victim required.
ERC-1400	Security token suite. Partitioned tokens, transfer agent certificates.	Implementation-level. CertificateController uses ecrecover to verify transfer agent signatures.	HIGH	Attacker authorizes unauthorized transfers of partitioned security tokens without issuer approval.

PRIMARY-SOURCE ANCHOR

ERC-2612's specification defines `permit(address owner, address spender, uint value, uint deadline, uint8 v, bytes32 r, bytes32 s)` and requires a valid `secp256k1` signature. That is why the standard cannot simply accept large post-quantum signatures without a replacement interface. See ERC-2612 and EIP-712.

> "If a user has made even one transaction, then the signature of that transaction reveals the public key."
>
> VITALIK BUTERIN, ETHEREUM FOUNDATION | ETHEREUM RESEARCH

ERC-3643: The Highest-Value Vulnerability in Institutional Crypto

ERC-3643 is the dominant institutional tokenization standard: $32B+ tokenized, 180+ jurisdictions, DTCC ComposerX integration, SEC endorsement, ISO standardization underway, 92+ association members. Its compliance enforcement depends on ONCHAINID, which verifies claim issuer signatures using ECDSA ecrecover. A quantum adversary forges a claim issuer signature, fabricates a KYC attestation, and any address appears compliant. $32 billion in regulated securities has its compliance gates bypassed. Migration requires a PQ-ONCHAINID variant. The chain upgrading does not fix ONCHAINID.

WHAT THIS MEANS FOR YOUR TOKENIZED PRODUCT

If you issued a regulated security on ERC-3643, the compliance layer that makes your product legal depends on ECDSA. A quantum adversary bypasses your compliance gates with one forged signature. Your tokenized bond, your fund shares, your structured product moves to an unauthorized wallet. This is not a protocol risk you can defer to Ethereum. This is a product risk on your issued securities. You must rebuild the identity verification layer underneath your product.

NAMED INSTITUTIONS EXPOSED VIA ERC-3643

DTCC | ABN AMRO | Apex Group ($3.5T AUA) | Invesco | Franklin Templeton | Fasanara Capital | 3iQ Corp | ZILO (Fidelity/State Street/Citi) | Zodia Custody (Std Chartered) | GLEIF | ANNA | BX Digital (Borse Stuttgart) | 21X (EU DLT Pilot) | Fireblocks | OpenZeppelin | Deloitte | A&O Shearman | Chainlink Labs | Ava Labs | Hedera Foundation | Solana Foundation | Plume Network | LayerZero Labs | Wormhole Foundation | tZERO | Tokeny/Apex Digital | Bitbond | ONYZE | BDACS | Halborn | Zama (FHE) | Inco | RedStone Oracles | EisnerAmper | +60 more members

ERC-2612: The Broadest Infrastructure Exposure

ERC-2612 hardcodes ECDSA into the standard specification. The permit function uses (uint8 v, bytes32 r, bytes32 s), which is ECDSA-specific. SPHINCS+ signatures (7,856-49,856 bytes) cannot fit. The standard cannot be adapted. It must be replaced.

Dollar exposure: USDC ($55B+), DAI/USDS (~$5B), stETH ($15B+), PYUSD, GHO, crvUSD, and all tokens deployed via OpenZeppelin ERC20Permit. Total permit token market cap exceeds $80B. Through Permit2, exposure extends to every ERC-20 on every EVM chain. Ethereum DeFi alone holds ~$38B TVL, nearly all routing through permit-dependent infrastructure.

WHAT THIS MEANS FOR YOUR STABLECOIN, CUSTODY INTEGRATION, AND DEFI YIELD PRODUCT

When Fireblocks processes a permit signature for an institutional USDC transfer, that signature is ECDSA. A quantum adversary forges it and drains the balance without the owner transacting. This is a custody risk, a fiduciary risk, and a regulatory risk. The standard cannot be adapted. Even after Ethereum hard forks to PQ transaction signing, your permit interface remains ECDSA-only. Your product remains vulnerable after the chain upgrades.

NAMED PLATFORMS EXPOSED VIA ERC-2612

Circle (USDC, $55B+) | MakerDAO/Sky (DAI, USDS) | PayPal (PYUSD) | Aave (aTokens) | Uniswap (UNI, Permit2) | 1inch | Compound | Lido (stETH) | Coinbase (cbETH) | Rocket Pool (rETH) | Frax Finance | Curve (crvUSD) | Fireblocks | Anchorage Digital | Coinbase Prime | Safe Global ($100B+ secured) | 0x Protocol | CoW Protocol | Across Protocol | Stargate/LayerZero | OpenZeppelin Defender | Biconomy | Gelato Network

Immutable Contracts: Permanent Quantum Vulnerability

Core DeFi infrastructure was deliberately made immutable so no administrator could alter behavior post-deployment. This design choice, which was correct for trust minimization, now creates permanent quantum vulnerability. These contracts collectively hold or route over $15 billion in TVL and serve as foundational infrastructure for the entire EVM ecosystem. They contain ECDSA logic (via ecrecover calls or hardcoded v/r/s permit signatures) that can never be replaced. They must be abandoned and redeployed as entirely new contracts on any PQ-safe chain.

CONTRACT	DEPLOYER	ECDSA DEPENDENCY	APPROX. TVL / IMPACT
Uniswap Permit2	Uniswap Labs	ecrecover for signature verification	Universal EVM approval layer
Uniswap V2 Pair	Uniswap Labs	ERC-2612 permit, hardcoded v/r/s	$2B+ TVL
Uniswap V3 Pool	Uniswap Labs	Immutable core	$3B+ TVL
Compound V2 cTokens	Compound Labs	ecrecover in governance	Multi-billion TVL
Curve Base Pools	Curve Finance	Immutable core logic	Multi-billion TVL
Balancer V2 Vault	Balancer	Immutable core	Multi-billion TVL
WETH9	Community	Immutable, no permit but foundational	$5B+ deposited
ENS Registry	ENS	Immutable	Ethereum naming infrastructure

WHAT THIS MEANS FOR YOUR INSTITUTIONAL VAULT AND DEFI YIELD PRODUCT

Institutional products do not exist in isolation from DeFi. BlackRock BUIDL uses ERC-4626 vaults. Those vaults interact with DeFi liquidity routing through Uniswap pools and Permit2. The institutional product and DeFi infrastructure are the same stack. When Permit2's ecrecover becomes forgeable, every token approval routed through it is compromised. These contracts cannot be upgraded. The only path is to deploy new contracts on PQ-safe infrastructure. EternaX offers this: the same institutional APIs (ERC-20, ERC-4626, ERC-4337) running on SPHINCS+ from day one, without inheriting Ethereum's immutable contract debt.

CHAIN 2 OF 3

Solana

PRIMARY-SOURCE ANCHOR

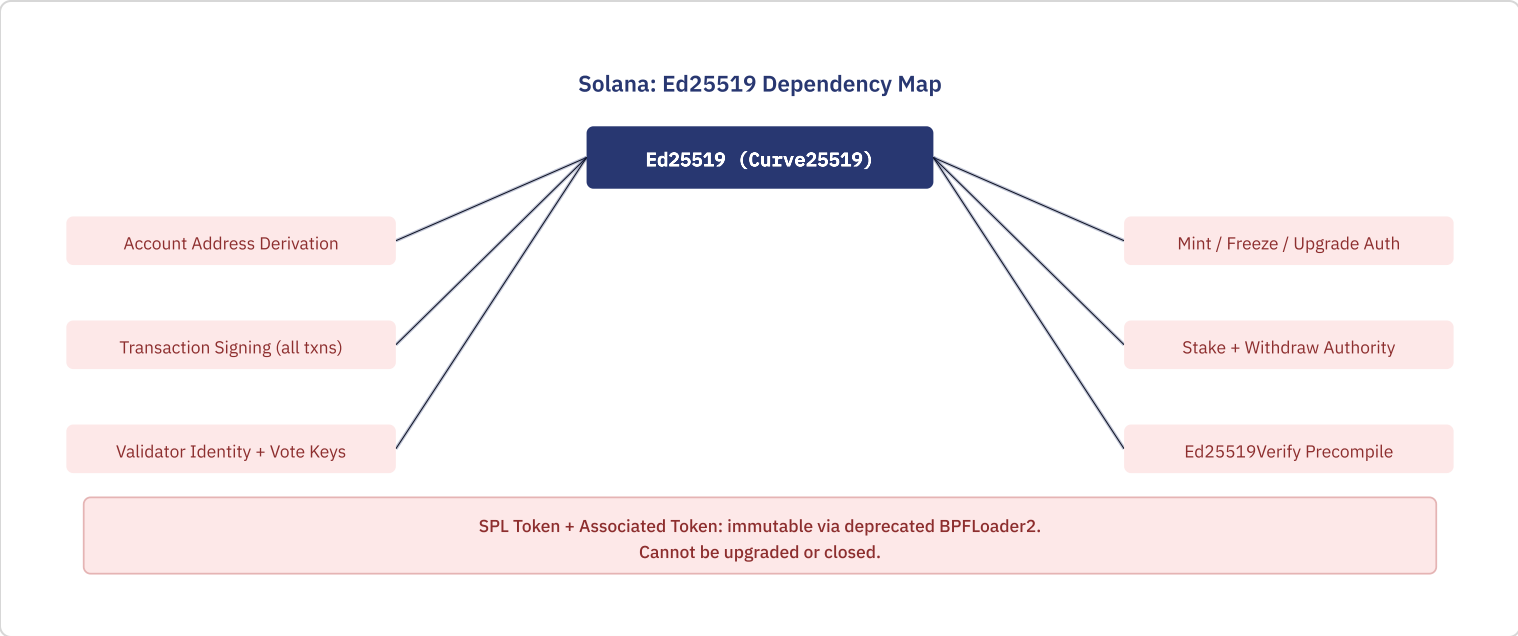
Solana documentation lists Ed25519, Secp256k1, and Secp256r1 signature verification as precompiled programs, and states that upgrade authority revocation makes a program immutable. See Solana Programs documentation.

"Using Shor's algorithms, factoring large numbers on a quantum computer would be just as fast as multiplication."

PETER SHOR, MIT | CERN INTERVIEW

Solana uses Ed25519 (Curve25519 elliptic curve) for every cryptographic operation on the chain. Ed25519 is equally vulnerable to Shor's algorithm as Ethereum's secp256k1 ECDSA. The vulnerability extends deeper on Solana because Ed25519 is not just the transaction signing scheme. It is the identity of every account, every authority key, every validator, and every governance surface on the network. Critically, Solana addresses are the raw 32-byte Ed25519 public keys themselves, not hashes of keys. Unlike Ethereum, where public keys are only revealed when an account first transacts, every Solana account's public key is permanently exposed on-chain from the moment of creation. There is no address-level quantum protection for any account on the network. Solana's DeFi ecosystem holds approximately $6-8 billion in TVL, with institutional products including Circle's USDC on Solana, BlackRock's BUIDL

(Solana class), Visa stablecoin settlement pilots, and WisdomTree tokenized funds all dependent on Ed25519 at every layer.



Native Precompiled Programs

Solana's Ed25519 and Secp256k1 verification programs are precompiled into the validator runtime as native code. They cannot be upgraded by any on-chain mechanism. Replacing them requires a coordinated validator software upgrade, equivalent to an Ethereum hard fork. Every on-chain program that uses these precompiles for custom authorization, including multisigs, custody schemes, and DeFi authorization logic, inherits quantum vulnerability and persists after any base protocol migration until individually updated.

GPU Signature Pipeline: Hardcoded for Ed25519

Solana's Transaction Processing Unit verifies Ed25519 signatures using GPU-accelerated CUDA kernels, achieving nearly one million verifications per second. The SigVerify stage sits on the critical path: no transaction can execute until its signatures are verified. The GPU pipeline is hardcoded for Ed25519 point arithmetic. Migrating to any PQ scheme requires entirely new GPU kernels with fundamentally different mathematical operations, introducing an engineering cost and performance unknown that no other chain faces at this scale.

SPL Token: Immutable Foundation

SPL Token and Associated Token are loaded by the deprecated BPFLoader2, making them permanently immutable. Every token on Solana, every stablecoin, every DeFi position depends on these programs. PQ migration requires deploying an entirely new token program and migrating all token state across the ecosystem.

Alpenglow Consensus: No PQ Equivalent

Solana's Alpenglow consensus uses BLS signature aggregation for validator voting. There is no post-quantum equivalent to BLS aggregation. Even if user transactions migrate to PQ, the consensus layer has an unsolved cryptographic problem.

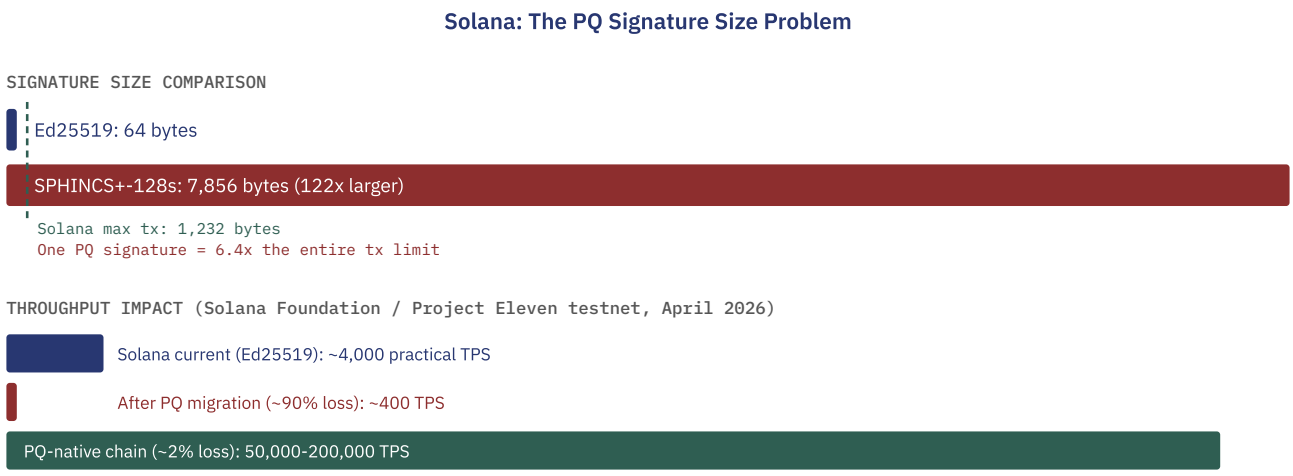
The Winternitz Vault: Not a Solution

Solana's only deployed PQ primitive is the Winternitz Vault: hash-based one-time signatures suitable for cold storage only. Each signature reveals ~50% of the private key. Not default. Users must opt in. Does not protect validator identities, consensus, transaction signing, DeFi programs, or any authority key. Critically, the Solana protocol requires a standard Ed25519 account to pay transaction fees. Vaults are user-defined programs that cannot pay fees directly. Anza's own research confirms: "Vaults alone are not sufficient because the account model is used to pay fees directly. Any fee payer account will be drainable if no action is taken to harden the account model." Even assets inside a vault require a quantum-vulnerable fee payer to access them.

Even If Solana Upgrades: The Performance Problem

In April 2026, the Solana Foundation and Project Eleven published testnet results from PQ signature trials. Post-quantum signatures tested were 20-40x larger than Ed25519. Project Eleven CEO Alex Pruden confirmed to CoinDesk that throughput declined by approximately 90%. The specific scheme was not publicly confirmed, but the 20-40x size range is consistent with NIST FIPS 204 (ML-DSA/Dilithium). Subsequently, both Anza and Firedancer converged on Falcon (FN-DSA, FIPS 206 track) as the preferred migration scheme, with smaller signatures (~10x Ed25519). But even with Falcon, a single signature plus public key (~1,563 bytes) exceeds Solana's current 1,232-byte transaction limit. The structural migration challenges, including transaction format overhaul, GPU pipeline rewrite, SPL Token immutability, consensus aggregation, fee model redesign, and hardware wallet support, persist regardless of scheme choice. No mainnet deployment exists. No timeline has been set. FIPS 206 (Falcon) is not yet finalized. No

hardware wallet, institutional custodian, or threshold-signing provider supports Falcon. A CBOM audit of Solana today reports Ed25519 as the deployed signing scheme.



Solana Foundation / Project Eleven testnet (April 2026): ~90% throughput decline under PQ signatures 20-40x larger than Ed25519. Even Falcon (~10x Ed25519) exceeds the current 1,232-byte transaction limit per signer. Source: CoinDesk, April 4, 2026.

> *The Solana Foundation confirmed in April 2026 that both Anza and Firedancer have converged on Falcon and published prototypes on GitHub. This is a roadmap, not a deployment. The institutional question is not whether Solana has a plan. It is whether your product can survive the gap between today's deployed Ed25519 cryptography and an unscheduled future migration across transaction format, account model, GPU verification pipeline, SPL Token, consensus, custody, and wallet infrastructure. EternaX absorbs the PQ performance cost at the architecture level (~2% TPS loss vs. ~90%) because it was designed around SPHINCS+ signature sizes from genesis, not retrofitted after deployment.*

NAMED PLATFORMS AND PROTOCOLS EXPOSED ON SOLANA

Raydium (largest DEX by TVL) · Orca (Whirlpools) · Jupiter (70%+ aggregator share) · Meteora · Phoenix (CLOB) · Marinade Finance · Jito · Drift Protocol · Marginfi · Kamino Finance · Phantom Wallet · Backpack Wallet · Solflare Wallet · Circle (USDC on Solana) · Visa (stablecoin settlement) · WisdomTree (tokenized funds) · BlackRock BUIDL (Solana class) · Pyth Network · Squads Protocol · Wormhole

CHAIN 3 OF 3

Canton Network

PRIMARY-SOURCE ANCHOR

Canton documentation lists Ed25519, ECDSA P-256, ECDSA P-384 for signing and ECIES on P-256 for asymmetric encryption. Canton security documentation states: "A namespace root signing key is a permanent key. It cannot be rotated without losing the namespace." Canton operations documentation states: "Every Synchronizer imposes a minimum set of cryptographic schemes. If a node does not support this minimum set of schemes, it is unable to connect." See Canton Security and Key Management and Canton Crypto Key Management.

> "A quantum adversary can not only decrypt future traffic but, if they want to, past traffic."
>
> SOFIA CELI AND NICK SULLIVAN, CLOUDFLARE | THE POST-QUANTUM FUTURE

Canton processes over $9 trillion per month in settlements across 700+ institutions including DTCC, Goldman Sachs, Broadridge, JPMorgan, HSBC, BNY Mellon, and Franklin Templeton. By settlement volume, it is the most consequential institutional blockchain in production. Its entire cryptographic stack is elliptic curve based. Zero post-quantum algorithms are deployed.

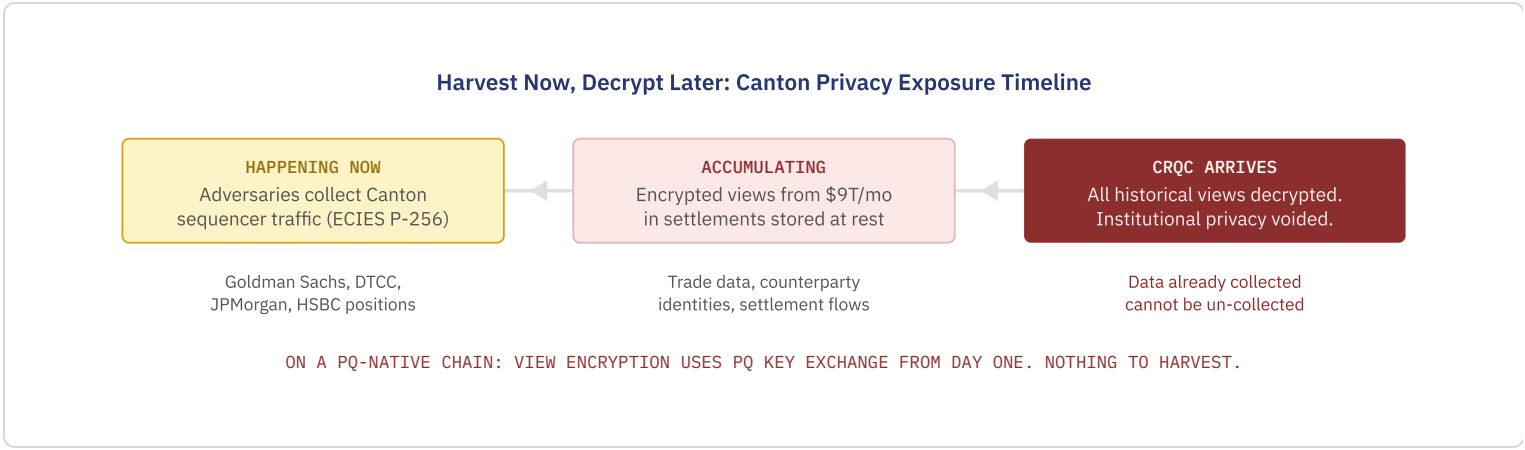
PRIMITIVE	SUPPORTED SCHEMES	QUANTUM STATUS	INSTITUTIONAL IMPACT
Signing	Ed25519 (default), ECDSA P-256, ECDSA P-384	ALL VULNERABLE	Six protocol layers: topology transactions, confirmation request Merkle root signing, confirmation response signing to mediator, transfer message signing, ACS commitment signing, and sequencer challenge-response authentication. Multi-view privacy multiplies the signature count per transaction across involved parties.
Asymmetric Encryption	ECIES on P-256 with HMAC-SHA256 and AES128-GCM	KEY EXCHANGE VULNERABLE	View encryption for sub-transaction privacy. Every encrypted view is decryptable once ECDLP is broken.
Symmetric Encryption	AES128-GCM	ADEQUATE	View content encryption. Secure if key exchange is PQ-safe. Currently compromised by vulnerable ECIES layer above.
MAC	HMAC with SHA-256	ADEQUATE	Message authentication. Not the primary risk surface.

The Harvest Now, Decrypt Later Problem

Canton's core value proposition is sub-transaction privacy, implemented using ECIES encryption on P-256. Every encrypted view ever sequenced through Canton's Global Synchronizer is stored with quantum-vulnerable keys. An adversary collecting sequencer traffic today decrypts every private transaction view

once a CRQC arrives. For a network whose institutional justification is privacy, this is a present-tense data collection opportunity for sophisticated adversaries.

> *Canton processes $9 trillion per month in institutional settlements. Every encrypted view from every settlement between Goldman Sachs, DTCC, JPMorgan, HSBC, Broadridge, and 700+ other institutions is decryptable under harvest-now-decrypt-later. The privacy guarantees that justify institutional participation are cryptographically time-limited.*



The Upgrade Path: Cleaner Application Layer, But Four Unsolved Protocol Problems

Canton's Daml abstraction layer means application contracts do not hardcode ECDSA in the way Ethereum's ERC-2612 or Uniswap Permit2 do. This is a genuine application-layer advantage. But the protocol layer, where signatures, encryption, identity, and consensus operate, faces structural migration challenges that are arguably harder than Ethereum's. As of June 2026, Digital Asset has published zero blog posts, zero documentation pages, zero GitHub activity, and zero conference presentations addressing post-quantum migration. For comparison: the Solana Foundation published a PQ readiness blog, testnet results, and multiple SIMDs. Ripple published a multi-phase XRPL PQ roadmap. Canton's public PQ posture consists of a CISO confirmation that the cryptographic API is extensible. For a network processing $9 trillion per month in institutional settlements, this silence is itself a material finding.

Problem 0: The Namespace Identity Impossibility

Canton's identity model permanently binds every namespace to the cryptographic fingerprint of its root signing key. Canton's own documentation states: "A namespace root signing key is a permanent key. It cannot be rotated without losing the namespace, as the namespace is identified by the fingerprint of the signing key. This is an architectural feature." Changing the root key from Ed25519 to a PQ scheme changes

the fingerprint, which changes the namespace, which destroys the identity. Every party, every node, every topology delegation, and every contract reference under that namespace breaks. This is not a coordination problem. It is a structural identity impossibility that must be solved before any of the migration challenges below become relevant.

Problem 1: ~88% Performance Collapse

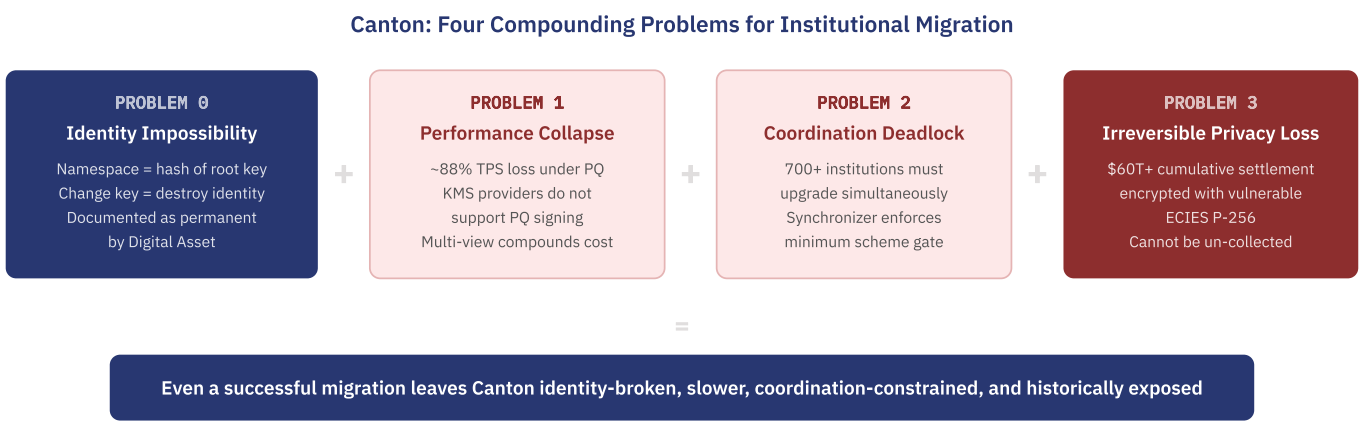
Replacing Ed25519 (64 bytes) with SPHINCS+ (7,856 bytes) inflates every signed message 122x. Canton's multi-view privacy model compounds this: every transaction view requires separate signing and encryption operations across all involved parties, multiplying the PQ penalty per transaction. For $9T/month in settlements, degraded throughput during migration creates systemic settlement risk. Additionally, Canton production deployments use AWS or GCP KMS for key management. Canton's documentation states that "Canton's supported schemes must match those provided by the KMS." Neither AWS KMS nor GCP KMS supports PQ signing (ML-DSA, SLH-DSA, or FN-DSA) as of June 2026. Even if Canton adds PQ support to its codebase, production institutional deployments cannot use PQ keys until cloud KMS providers add support.

Problem 2: 700+ Institutions Must Coordinate Simultaneously

Canton's privacy model requires all parties to agree on the cryptographic scheme. Partial migration breaks atomic settlement. Canton's Synchronizer enforces this technically: the documentation states that every Synchronizer imposes a minimum set of cryptographic schemes, and any node that does not support the required set is unable to connect. Partial migration is not merely organizationally difficult. It is architecturally impossible. Goldman Sachs, DTCC, JPMorgan, HSBC, Broadridge, and 690+ others must upgrade to PQ simultaneously, or the classical scheme remains the operating standard and no quantum safety is achieved. No precedent exists for coordinated cryptographic migration across this many regulated institutions.

Problem 3: The Privacy Damage Is Already Done

Even perfect future migration cannot protect $60T+ in cumulative settlement volume already encrypted with quantum-vulnerable ECIES P-256. Every trade, every position, every counterparty relationship settled on Canton is retrospectively exposed. Upgrading protects future transactions. It does not protect the past.



PQ-native infrastructure eliminates all four problems: identity is PQ from genesis, performance is architected for PQ from day one (~2% loss), no legacy participants require coordination, and no historical data is encrypted with vulnerable keys.

Canton's four unsolved problems compound: the namespace identity model permanently binds every party and node to classical keys, the performance penalty degrades throughput by ~88% while cloud KMS providers do not yet support PQ signing, the coordination challenge spans 700+ institutions enforced by a Synchronizer scheme gate that makes partial migration technically impossible, and the privacy damage to $60T+ in historical settlements is irreversible. Institutions choosing settlement infrastructure today face a question: build on rails where all four problems must be solved simultaneously, or build on EternaX, where PQ-native signing, encryption, and identity are solved at genesis and none of the four problems exist.

NAMED INSTITUTIONS EXPOSED ON CANTON NETWORK

DTCC ($100T+ custody base) · Goldman Sachs (GS DAP) · Broadridge ($350B+ daily repo) · JPMorgan · HSBC · BNY Mellon · Deutsche Borse · Franklin Templeton (Benji) · Paxos · CBOE · Deloitte · Microsoft · Moody's · Capgemini · BNP Paribas · Digital Asset (protocol builder) · Canton Foundation / GSF · Euroclear (co-chair) · 700+ total participants

> "If quantum computing becomes a threat to Bitcoin's elliptic curve cryptography, an inviolable property of Bitcoin will be violated one way or another."
>
> JAMESON LOPP, BITCOIN SECURITY RESEARCHER | AGAINST ALLOWING QUANTUM RECOVERY OF BITCOIN

INSTITUTIONAL RESPONSE FRAMEWORK

What Institutions Should Do Now

The evidence in this report points to four immediate actions for any institution issuing, holding, or custodying digital assets on Ethereum, Solana, or Canton.

ACTION	WHY NOW	WHO OWNS IT
1. Conduct a cryptographic inventory	Federal PQC guidance requires cryptographic inventory and migration planning for high-assurance systems. Institutional products on public blockchains must enumerate: which signing scheme secures each asset, which standards embed ECDSA in their specification or implementation, which contracts are immutable, and which custody integrations depend on permit flows.	CISO / CTO
2. Assess application-layer PQ exposure	Chain-layer upgrades do not fix application-layer problems. Institutions must separately assess: ERC-3643 ONCHAINID claim verification, ERC-2612 permit interface dependencies, immutable contract dependencies in DeFi routing, and custody platform signature schemes. Each of these persists after any chain upgrade.	CTO / Engineering
3. Evaluate PQ-native settlement rails	For new issuance and long-duration tokenized products (bonds, fund shares, structured credit), the cost of issuing onto quantum-vulnerable rails today is the guaranteed migration debt tomorrow. PQ-native chains eliminate this debt at issuance. The evaluation criteria: native PQ signing (not optional vaults), institutional-grade throughput under PQ (~2% loss, not ~90%), and day-one compatibility with ERC-20/ERC-721/ERC-4626/ERC-4337.	Product / Strategy
4. Engage custodians on CBOM readiness	Custodians subject to federal mandates will be required to justify the cryptographic posture of every asset they custody. If your custodian cannot answer the CBOM question for your product's underlying chain, your product faces restriction or restructuring. Start the conversation now, not when the FAR amendment takes effect.	Operations / Compliance

For Action Item 3, EternaX offers a practical next step: a chain-aware CBOM exposure review for tokenized funds, stablecoins, custody stacks, settlement workflows, and DeFi integrations, followed by a PQ-native issuance path using the same institutional APIs institutions already use.

PQ-NATIVE MARKET INFRASTRUCTURE

EternaX: Institutional Rails That Do Not Require Repair

For institutions evaluating post-quantum settlement rails, EternaX is PQ-native market infrastructure for stablecoin issuance, RWA tokenization, custody-adjacent workflows, and institutional settlement. The premise is simple: do not inherit cryptographic debt that must be repaired later. Every layer documented in this report as non-upgradeable on existing chains is addressed at genesis: accounts, signatures, verifier logic, identity, permits, compliance modules, and settlement assumptions.

STANDARDS ANCHOR

EternaX's PQ-native signature posture is anchored to NIST-recognized post-quantum standards, especially FIPS 205 / SLH-DSA, which specifies a stateless hash-based digital signature algorithm based on SPHINCS+.

The primary defense is SPHINCS+ (NIST FIPS 205, SLH-DSA), a hash-based signature standard whose security reduces to well-understood hash function properties. SPHINCS+ is not an add-on or optional feature. It is the native signing scheme at the protocol level. Every address, every transaction, every precompile, every consensus attestation uses PQ-safe cryptography from the first block.

Performance Under Post-Quantum Cryptography

The institutional objection to PQ is performance. SPHINCS+ signatures are 122x larger than ECDSA. Every existing chain that attempts PQ migration faces severe throughput penalties. EternaX absorbs this cost at

the architecture level.

50K-200K	20-50ms	400-520ms	~2%
Transactions per second	Soft finality	Hard finality	TPS loss under PQ

The ~2% cost results from architectural decisions at the protocol design stage. Consensus is designed from genesis to handle PQ signature sizes efficiently. A compact permanent receipt layer reduces per-transaction storage by 49x (160 bytes vs 7,856 bytes). Existing chains face ~84-90% loss. The difference between ~2% and ~90% is the difference between a chain institutions can use and one they cannot.

Solana (PQ retrofit)	~90% TPS loss
Ethereum (PQ retrofit)	~84% TPS loss
Canton (PQ retrofit)	~88% TPS loss
EternaX (PQ-native)	~2% TPS loss

Same Institutional APIs. PQ-Native with SPHINCS+.

Institutions do not need to learn new standards. EternaX provides the same facilities they already use for compliance, permits, security tokens, vaults, and programmable custody, running on PQ-native rails that will never need to be ripped out.

TIER	STANDARDS	WHAT THE INSTITUTION SEES	WHAT CHANGES UNDERNEATH
Tier 1: Deploy unchanged	ERC-20, ERC-721, ERC-4626, ERC-4337, ERC-7943	Identical API. Same functions, same parameters, same integration code. Zero learning curve.	SPHINCS+ operates at the transaction layer. The institution never touches the cryptography.
Tier 2: Same API, PQ module	ERC-3643, ERC-1400	Same ONCHAINID concept, same claim topics, same trusted issuers, same compliance flow. Same CertificateController interface.	isClaimValid verifies with SPHINCS+ instead of ecrecover. Certificate signatures verified with SPHINCS+. Interface identical.
Tier 3: PQ-native redesign	ERC-2612 replacement	Same facility: gasless approvals, off-chain authorization. Custody platforms authorize token movements without on-chain transactions.	New PQ-permit interface with bytes signature parameter accepting SPHINCS+. **Whoever ships this first defines the standard.**

> *The question for institutions is not when a quantum computer will arrive. The question is: why are you still issuing long-duration value onto rails that guarantee avoidable future migration debt, when the same institutional APIs exist on PQ-native infrastructure today?*

ENTITY GLOSSARY

Key Entities and Definitions

EO 14412

U.S. Executive Order titled "Securing the Nation Against Advanced Cryptographic Attacks." It directly binds federal agencies and creates a private-sector cascade through procurement, contractors, regulated clients, CBOM disclosure, and vendor diligence.

CBOM

Cryptographic Bill of Materials. A machine-readable inventory of cryptographic algorithms, libraries, keys, standards, and dependencies used by a system or product.

ECDSA

Classical elliptic-curve signature scheme used by Ethereum, Bitcoin, and many institutional custody flows. It is vulnerable to Shor's algorithm once public keys are exposed.

Ed25519

Edwards-curve signature scheme used across Solana, Stellar, and Canton defaults. It is not post-quantum secure and appears across account, validator, and authority models.

ECIES P-256

Classical elliptic-curve encryption scheme used in privacy-sensitive systems. Historical encrypted traffic can remain exposed to harvest-now-decrypt-later attacks.

ERC-3643

Regulated token standard for permissioned securities and tokenized assets. Its ONCHAINID claim verification can inherit ECDSA-based compliance exposure.

ERC-2612

Permit approval standard with ECDSA-shaped v, r, s signature parameters. It cannot directly encode large post-quantum signatures without a replacement interface.

SLH-DSA / SPHINCS+

NIST-standardized stateless hash-based post-quantum signature scheme under FIPS 205. EternaX uses this family as its conservative PQ-native signing anchor.

SPL Token

Core Solana token program used for fungible assets, mint authority, freeze authority, and token account control. Its authority model depends on Ed25519.

Canton Namespace

Canton identity construct tied to the fingerprint of a root signing key. This creates a hard migration

problem if the root key must move from classical to PQ cryptography.

CLAIMS AND SOURCES

Machine-Readable Evidence Map

REPORT CLAIM	PRIMARY SOURCE	WHY IT MATTERS
NIST has standardized SLH-DSA as a stateless hash-based post-quantum signature standard.	NIST FIPS 205 / SLH-DSA	Anchors the EternaX conservative PQ-signature posture to an official NIST standard.
EO 14412 makes PQC migration a direct federal priority and creates contractor, procurement, and CBOM pressure.	Federal Register: EO 14412	Turns PQC from future planning into board-level compliance and vendor-risk diligence.
ERC-2612 is structurally ECDSA-shaped through v, r, s permit parameters.	Ethereum EIP-2612	Explains why existing permit interfaces cannot simply accept large PQ signatures.
EIP-712 typed-data signing supports permit, custody, and institutional authorization flows that depend on classical signature verification.	Ethereum EIP-712	Shows how transaction authorization and offchain approvals inherit the same cryptographic base.
Solana exposes signature-verification primitives at the runtime and program layer.	Solana Program Documentation	Supports the claim that Solana's exposure is not limited to wallet signing.
Canton documents classical signing and encryption scheme support, including Ed25519, ECDSA, and ECIES.	Canton Security and Key Management	Supports the report's claim that Canton has signing, identity, and privacy-layer PQ migration challenges.
Ethereum public keys become exposed after an account transacts, making active accounts materially different from dormant addresses in a PQ world.	Ethereum Research: Quantum Emergency	Explains why active institutional admin, treasury, custody, and signer keys need special treatment.
Public agencies recommend preparing cryptographic inventories and migration plans before a cryptographically relevant quantum computer arrives.	CISA, NIST, and NSA PQC Guidance	Supports the report's CBOM-first action framework for institutions.

PRIMARY SOURCE REGISTER

Evidence Base

CLAIM FAMILY	PRIMARY SOURCE	WHY IT MATTERS
NIST PQC standards	NIST finalized PQC standards, FIPS 205 / SLH-DSA	Confirms finalized PQC standards and the hash-based SLH-DSA signature standard.
U.S. national-security PQC transition	NSA CNSA 2.0 announcement	Confirms official quantum-resistant algorithm requirements for National Security Systems.
Ethereum permit exposure	ERC-2612, EIP-712	Confirms the v/r/s and secp256k1 structure of permit-based approvals.
Solana runtime exposure	Solana Programs documentation	Confirms precompiled signature verification programs and immutability after upgrade authority revocation.
Canton signing and encryption exposure	Canton Security and Key Management	Confirms Ed25519, ECDSA P-256/P-384, and ECIES P-256 schemes in Canton documentation.

CLAIM FAMILY	PRIMARY SOURCE	WHY IT MATTERS
Quantum threat and migration urgency	Michele Mosca, IACR ePrint, CISA, NIST, and NSA guidance, NIST IR 8547	Confirms that today's public-key cryptography must migrate and that migration should begin before CRQC arrival.
Ethereum public-key exposure	Vitalik Buterin, Ethereum Research	Confirms that a single transaction reveals the public key, making transacted EOAs exposed in a post-quantum world.
Harvest-now-decrypt-later and crypto governance	Cloudflare post-quantum future, Jameson Lopp on quantum recovery, CERN interview with Peter Shor	Supports the report's claims on stored encrypted-data exposure, elliptic-curve migration tradeoffs, and Shor's algorithm risk.

CONTINUE ETERNAX RESEARCH

For deeper diligence, read the **Post-Quantum Signature Security Ranking 2026**, the **PQC Risk Framework for Institutions**, the **PQ Exposure Map for Institutional Crypto and Tokenized Assets**, and **Why EternaX**.

Frequently Asked Questions

Optimized for institutional diligence, search discovery, and direct answers on Ethereum, Solana, Canton, custody, tokenization, and PQ-native migration.

Can quantum computers break blockchain?

Yes. Quantum computers running Shor's algorithm can derive private keys from public keys for any blockchain using ECDSA or Ed25519, including Ethereum, Solana, Canton, Stellar, and Bitcoin. This means forging signatures, stealing assets, impersonating validators, and bypassing compliance gates. Google Quantum published circuits in 2026 requiring fewer than 500,000 physical qubits to break ECDSA P-256. Oratomic estimated as few as 10,000-20,000 qubits on neutral-atom architecture. EternaX is the only institutional blockchain built on NIST-approved post-quantum cryptography (SPHINCS+/FIPS 205) from genesis.

When will quantum computers break Bitcoin and Ethereum?

No one knows the exact date, but the timeline is compressing. Anza (Solana's core team) assigns a 3-5% probability of breaking ECDLP-256 within five years as of April 2026. Google Quantum published circuits requiring 20x fewer qubits than previous estimates. The relevant institutional risk is harvest-now-decrypt-later: adversaries collecting encrypted data and signed transactions today for decryption later. Canton's $60T+ in encrypted settlement views and every exposed public key on Ethereum and Solana are already at risk of collection. EO 14412 sets federal PQC compliance deadlines of 2030-2031 because the U.S. government considers the threat actionable now.

Which blockchain is quantum resistant in 2026?

As of June 2026, no major L1 blockchain has deployed post-quantum cryptography as its default signing scheme. Ethereum uses ECDSA. Solana uses Ed25519. Canton uses Ed25519 and ECDSA P-256. Bitcoin uses ECDSA. All are quantum-vulnerable. Solana has Falcon prototypes but no mainnet deployment. Ethereum has EIP-8141 proposed but no deployment. Canton has zero public PQ documentation. EternaX is the only institutional blockchain using NIST-approved post-quantum signatures (SPHINCS+/SLH-DSA, FIPS 205) as its deployed signing scheme, with ~2% TPS loss versus ~84-90% for retrofitted chains.

Is Bitcoin quantum safe?

No. Bitcoin uses ECDSA on secp256k1 for transaction signing. ECDSA is vulnerable to Shor's algorithm. Addresses that have ever spent (exposing the public key) are directly vulnerable. Pay-to-public-key addresses, including early Satoshi-era coins, have permanently exposed public keys. There is no consensus on a Bitcoin PQ migration path, no BIP proposing PQ signatures, and no timeline. NIST IR 8547 classifies ECDSA as deprecated after 2030 and disallowed after 2035. A CBOM audit of Bitcoin today returns FAIL.

What is SPHINCS+ and why is it used for post-quantum blockchain?

SPHINCS+ is a hash-based digital signature scheme standardized by NIST as FIPS 205 (SLH-DSA) in August 2024. It is considered the most conservative post-quantum signature scheme because its security relies only on hash functions, not on lattice assumptions or newer mathematical structures. SPHINCS+ signatures are larger than classical signatures (7,856 bytes vs. 64 bytes for Ed25519), but a PQ-native chain like EternaX architects around this from genesis, absorbing the size at ~2% TPS loss. Chains retrofitting SPHINCS+ after deployment face ~84-90% throughput decline because their transaction formats and verification pipelines were designed for small classical signatures.

Will Solana's Falcon upgrade make it fully quantum safe?

No. Falcon would address transaction signing if deployed, but Solana's quantum exposure extends far beyond signing. SPL Token is permanently immutable via BPFLoader2. The GPU pipeline is hardcoded for Ed25519 CUDA. Addresses are raw public keys with zero address-level protection. Alpenglow consensus uses BLS aggregation with no PQ equivalent. Every program using Ed25519 precompiles inherits vulnerability. The Winternitz Vault cannot protect fee payer accounts. FIPS 206 (Falcon) is not yet finalized. No hardware wallet supports Falcon. No mainnet deployment exists. No timeline has been set.

Can blockchain be upgraded to be quantum safe?

Only partially, and not within institutional planning horizons. A chain can upgrade its consensus-layer signing, but that does not fix immutable contracts (Uniswap Permit2, Compound V2, WETH9 on Ethereum), frozen token standards (ERC-2612 with hardcoded ECDSA), immutable programs (SPL Token on Solana), namespace identity locked to classical keys (Canton), historical encrypted settlement data (Canton ECIES), or custody integrations built on classical signing. Ethereum's full execution-layer migration is estimated at years beyond its ~2029 L1 target. Solana has Falcon prototypes but no mainnet or timeline. Canton has zero public PQ roadmap. For new issuance, PQ-native infrastructure like EternaX eliminates migration debt entirely by building on SPHINCS+ from genesis.

Will Ethereum, Solana, or Canton post-quantum roadmaps fix institutional products automatically?

No. A chain roadmap can address part of the protocol layer, but it does not automatically fix products already built on top of that chain. On Ethereum, ERC-3643 ONCHAINID can continue verifying ECDSA claim signatures, ERC-2612 permit can remain locked to v/r/s ECDSA parameters, and immutable contracts such as Uniswap Permit2, Compound V2, WETH9, and Curve base pools can remain permanent. On Solana, SPL Token remains immutable through the deprecated BPFLoader2, and existing authority models still depend on Ed25519. On Canton, historical ECIES P-256 encrypted views remain retrospectively exposed. The institutional decision is therefore not, will the chain eventually migrate. The decision is whether your product can survive the parts that do not migrate.

What U.S. federal post-quantum requirements should crypto institutions track?

Institutions should track NSM-10, OMB M-23-02, the Quantum Computing Cybersecurity Preparedness Act, NSA CNSA 2.0, CISA/NSA/NIST quantum-readiness guidance, NIST FIPS 203/204/205, and Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks." EO 14412 directly binds federal agencies, then propagates pressure through contractors, procurement, regulated clients, vendor diligence, and CBOM disclosure. For blockchain products, the required inventory must be chain-aware: signature scheme, address model, precompiles, standards, custody signing flows, encrypted settlement data, and immutable contracts.

What is Executive Order 14412 and why does it matter for digital assets?

Executive Order 14412, "Securing the Nation Against Advanced Cryptographic Attacks," was signed on June 22, 2026 and published in the Federal Register. It directly sets federal PQC migration obligations and creates a private-sector cascade through federal procurement, contractors, regulated clients, custody providers, settlement vendors, and CBOM disclosure. For digital assets, the key point is simple: future diligence will ask what cryptography is deployed today, not what a chain hopes to upgrade later.

What are the key deadlines in Executive Order 14412?

Within 30 days (July 2026): each agency names a PQC migration lead. Within 90 days (September 2026): OMB issues binding guidance requiring cryptographic inventory and migration plans. Within 180 days (December 2026): FAR Council publishes proposed rule requiring federal contractors to comply with NIST FIPS PQC by December 31, 2030. Within 270 days (~March 2027): CISA and NIST publish CBOM guidance for machine-readable cryptographic inventories. December 31, 2030: federal agencies implement PQC for key establishment on high-value assets; federal contractors achieve full NIST FIPS PQC compliance. December 31, 2031: federal agencies implement PQC for all digital signature systems. 2035: NIST IR 8547 fully disallows ECDSA, RSA, and EdDSA, including legacy systems.

How does Executive Order 14412 reach private-sector blockchain and custody infrastructure?

Through procurement, contractors, CBOM disclosure, critical-infrastructure resilience expectations, regulated-client diligence, and vulnerability-disclosure obligations. EO 14412 does not automatically bind every private blockchain company, but it gives federal agencies, contractors, banks, custodians, and settlement providers a clear reason to demand cryptographic inventories and NIST-aligned PQ migration plans from vendors.

Do Ethereum, Solana, Canton, or Stellar pass a CBOM post-quantum audit today?

No. A CBOM audit reports what is deployed, not what is on a roadmap. As of June 2026, Ethereum uses ECDSA (secp256k1), Solana uses EdDSA (Ed25519), Canton uses Ed25519 and ECDSA P-256, and Stellar uses EdDSA (Ed25519). All are deprecated or disallowed under NIST IR 8547 by 2035. None has a NIST-approved post-quantum signature scheme deployed in production. A CBOM audit of any of these chains returns a compliance gap for every transaction signing, custody authorization, and settlement operation. A PQ-native chain using SPHINCS+ under NIST FIPS 205 passes the same audit from day one.

Can Ethereum hard fork to post-quantum cryptography and fully fix ECDSA exposure?

Not fully. A hard fork can change future protocol rules, but it cannot retroactively make existing application-layer infrastructure quantum safe. Ethereum has five layers of ECDSA exposure: address derivation, transaction signing, the ecrecover precompile, immutable smart contracts, and frozen permit interfaces. Address derivation exposes public keys once an EOA transacts. Transaction signing requires coordination across clients, validators, wallets, L2s, and infrastructure providers. ecrecover is a protocol-level primitive. Immutable contracts cannot be patched. ERC-2612 permit interfaces cannot accept PQ signatures because their ABI is ECDSA-specific. A hard fork may protect part of future transaction validation, but it does not rewrite the institutional application stack.

Why does one Ethereum transaction create post-quantum exposure?

An Ethereum externally owned account is derived from a secp256k1 public key. Before an account sends its first transaction, the public key is not visible onchain, only the address is visible. Once the account signs and sends a transaction, the signature reveals enough information for the public key to be recovered. Under classical assumptions this is acceptable. Under a cryptographically relevant quantum computer, elliptic-curve public keys become a path to private-key recovery through Shor's algorithm. That means any Ethereum address with an exposed public key becomes materially different from a never-used address. For institutions, this matters because operational wallets, admin keys, signer keys, custody keys, and treasury addresses are usually active, not dormant.

Is ERC-3643 quantum safe?

No. ERC-3643 is not quantum safe because its compliance layer depends on ONCHAINID claim verification using ECDSA. The critical function is isClaimValid, which verifies claim issuer signatures through ecrecover on secp256k1. If a quantum adversary can derive a claim issuer private key from an exposed public key, they can forge KYC, AML, accreditation, jurisdiction, or investor-eligibility attestations. The consequence is not theoretical. A regulated security token can treat an ineligible wallet as compliant because the compliance proof itself has been forged. This is one of the highest-severity institutional vulnerabilities because ERC-3643 exists specifically to enforce regulated transfer restrictions.

How does the ONCHAINID ECDSA vulnerability break ERC-3643 compliance?

ONCHAINID is the identity and claim system used by ERC-3643 to decide whether a wallet is eligible to receive a regulated token. When a transfer occurs, the token's identity registry checks whether the recipient has the required claims from trusted issuers. Those claims are cryptographically signed. In the current architecture, claim signatures are verified using ECDSA ecrecover. A quantum attacker who recovers or forges a trusted issuer's signing key can create fraudulent claims that appear valid onchain. The token does not need to be hacked directly. The compliance gate is bypassed because the identity proof has been forged. A post-quantum migration therefore requires a PQ-ONCHAINID design, not only an Ethereum hard fork.

Which institutions are exposed through ERC-3643 and ONCHAINID?

The ERC3643 Association has 92+ confirmed members and reaches directly into regulated tokenization. Relevant exposed entities include DTCC through ComposerX integration, ABN AMRO through digital bond issuance, Apex Group through Tokeny, Invesco, Franklin Templeton, Fasanara Capital, 3iQ Corp, Zodia Custody, GLEIF, BX Digital, 21X, Fireblocks, OpenZeppelin, Deloitte, A&O Shearman, Chainlink Labs, Ava Labs, Hedera Foundation, Solana Foundation, Plume Network, LayerZero Labs, Wormhole Foundation, tZERO, Bitbond, ONYZE, BDACS, Halborn, Zama, Inco, and RedStone. The relevant question is not whether these institutions are insecure today. The question is whether their regulated-token infrastructure inherits ECDSA-based compliance verification that cannot become quantum safe without redesign.

Can ERC-2612 permit be upgraded for post-quantum signatures?

No. ERC-2612 permit is structurally incompatible with post-quantum signatures because the standard hardcodes ECDSA-specific parameters into the function interface: uint8 v, bytes32 r, and bytes32 s. SPHINCS+ and other PQ signature schemes do not decompose into v/r/s and can be thousands of bytes long. A proxy upgrade can change logic behind a contract, but it cannot safely change a widely integrated ABI without breaking downstream callers. Wallets, aggregators, custody platforms, DEX routers, and institutional policy engines already expect the existing permit interface. The clean migration is a new PQ-permit interface using a generic bytes signature and explicit verifier logic.

Can a stablecoin issuer make ERC-2612 post-quantum safe without replacing permit?

Not fully. A stablecoin issuer can add new contract logic, restrict certain flows, or launch a new token version, but the existing ERC-2612 permit interface remains ECDSA-shaped. The issue is not only the verifier. The interface itself cannot physically accept a PQ signature in the form required by schemes such as SPHINCS+. For USDC, DAI, PYUSD, and other permit-enabled assets, the institutional risk is that approvals can be forged once ECDSA becomes breakable and the relevant public key is exposed. The durable solution is a replacement PQ-permit standard, updated wallet support, updated custody workflows, and migration of liquidity integrations.

Is USDC quantum safe on Ethereum or Solana?

No. USDC on Ethereum inherits ERC-2612 permit exposure through an ECDSA-specific interface, and USDC on Solana depends on Solana's Ed25519 account and authority model plus SPL Token infrastructure. Circle can upgrade some contract logic on Ethereum through proxy patterns, but it cannot make the frozen permit ABI accept PQ signatures without a new interface and downstream integration migration. On Solana, the SPL Token program is immutable and authority keys are Ed25519. For an institutional holder, the risk is not that USDC fails today. The risk is that the stablecoin's rails depend on cryptographic assumptions that are not post-quantum safe and cannot be repaired cleanly in place.

Is Uniswap Permit2 quantum safe?

No. Uniswap Permit2 is an immutable approval contract that uses ECDSA recovery for signature verification. It has no proxy pattern, no admin key, and no upgrade function. It is a widely used approval layer across EVM DeFi, including aggregators, routers, custody workflows, and institutional transaction systems. Once ECDSA becomes breakable for exposed public keys, forged approvals become possible wherever Permit2 verification remains trusted. The important institutional point is that Permit2 cannot be patched in place. It must be abandoned, replaced, and reintegrated. That is a migration of ecosystem behavior, not a simple protocol upgrade.

Are immutable smart contracts quantum vulnerable forever?

Yes, if their security logic depends on ECDSA, Ed25519, or another quantum-vulnerable primitive. Immutable contracts and immutable programs cannot be patched because their code is final. On Ethereum, relevant examples include Uniswap Permit2, Uniswap V2 and V3 pools, Compound V2, Curve base pools, Balancer V2 Vault, WETH9, and ENS Registry. On Solana, SPL Token and Associated Token are immutable through the deprecated BPFLoader2. The solution is not upgrading those contracts. The solution is replacement deployments, migration of integrations, and user or institutional movement to new rails. On a PQ-native chain, this legacy immutable-contract debt does not exist at genesis.

What should an ERC-3643 issuer do now about post-quantum risk?

An ERC-3643 issuer should start with a chain-aware cryptographic inventory. The issuer should identify every ONCHAINID claim issuer, every trusted issuer key, every ecrecover dependency, every wallet and custody policy that signs or verifies claims, and every downstream transfer restriction that depends on classical signatures. Then it should define a PQ-ONCHAINID migration path, including PQ claim signatures, expanded key types, new verifier contracts, migration rules for existing identities, and a plan for new issuance on infrastructure that does not inherit ECDSA verification. For new regulated products, the cleanest path is not to issue into avoidable cryptographic debt. It is to use PQ-native rails where identity, signing, and verification are designed for post-quantum requirements from day one.

Is Solana quantum resistant or vulnerable to Ed25519 quantum attacks?

Solana is vulnerable to quantum attacks against Ed25519. Ed25519 is used for transaction signing, account authority, mint authority, freeze authority, program upgrade authority, validator identity, vote authority, stake authority, and withdraw authority. Solana addresses are the raw 32-byte Ed25519 public keys, not hashes, meaning every account's public key is permanently exposed on-chain from creation. The GPU signature verification pipeline is hardcoded for Ed25519 CUDA kernels. SPL Token is immutable. In April 2026, the Solana Foundation and Project Eleven published testnet results showing ~90% throughput decline under PQ signatures. Both Anza and Firedancer subsequently converged on Falcon (FN-DSA), but no mainnet deployment exists, no timeline has been set, and no hardware wallet or institutional custodian supports Falcon. A CBOM audit of Solana today reports Ed25519 as the deployed signing scheme.

Can Solana's Winternitz Vault protect users from quantum attacks?

Only in a narrow cold-storage use case. A Winternitz Vault uses hash-based one-time signatures, which can reduce exposure for assets held with very low signing frequency. It is optional, not default. It is one-time-use, meaning the user must rotate to a new vault after signing. It does not protect validator identities, vote keys, stake authorities, program upgrade authorities, DeFi programs, SPL Token authority models, or ordinary account signing. Critically, the Solana protocol requires a standard Ed25519 account to pay transaction fees. Vaults cannot pay fees directly. Anza's own research confirms that any fee payer account remains drainable if the account model is not hardened. Even assets inside a vault require a quantum-vulnerable fee payer to access them. It is not a system-wide post-quantum migration for Solana.

Is Solana SPL Token permanently exposed to post-quantum risk?

SPL Token is structurally difficult to repair because it is immutable through the deprecated BPFLoader2 path and cannot simply be upgraded like a modern program. SPL Token also sits at the base of Solana's token economy. Mint authorities, freeze authorities, token accounts, and associated token flows depend on Ed25519 authority models. A new token program could be created, but that would require assets, issuers, wallets, exchanges, DeFi protocols, custody platforms, and infrastructure providers to migrate. That is not a patch. It is an ecosystem migration. For institutional Solana issuers, the key question is whether future issuance should continue inheriting this authority model or move to PQ-native infrastructure.

Does Solana Alpenglow solve post-quantum security?

No. Alpenglow is a consensus-performance redesign, not a full post-quantum security migration. The relevant concern is that modern high-performance consensus systems often depend on aggregation and compact signatures, and BLS-style aggregation has no clean, practical post-quantum equivalent with the same operational profile. Even if Solana improves finality and consensus performance, that does not automatically fix Ed25519 transaction signing, account authority, SPL Token immutability, precompiled runtime behavior, or application-layer authority keys. For institutions, Alpenglow may improve speed, but speed does not equal post-quantum safety.

Is Canton Network quantum resistant or post-quantum safe?

No. Canton relies on classical elliptic-curve cryptography at every protocol layer. Zero post-quantum algorithms are deployed. Canton's namespace identity model permanently binds every party and node to the fingerprint of a classical root signing key, which Canton's own documentation states cannot be rotated without losing the namespace. Its Synchronizer enforces a minimum cryptographic scheme set, making partial migration technically impossible. As of June 2026, Digital Asset has published zero public PQ documentation, roadmaps, or implementations, despite processing $9 trillion per month in institutional settlements.

What is Canton's namespace identity problem for post-quantum migration?

Canton's identity model derives every namespace from the hash of a root signing key's fingerprint. Canton's own documentation states: "A namespace root signing key is a permanent key. It cannot be rotated without losing the namespace, as the namespace is identified by the fingerprint of the signing key. This is an architectural feature." Changing from a classical key to a PQ key changes the fingerprint, which changes the namespace, which destroys the identity. Every party, every node, every topology delegation, and every contract reference under that namespace breaks. This is not a coordination problem. It is a structural identity impossibility documented by Digital Asset themselves. It must be solved before performance, coordination, or privacy migration can even be attempted.

What is Canton Network's harvest-now-decrypt-later risk?

Canton's value proposition is sub-transaction privacy. That privacy depends on encrypted transaction views. If those views are protected with ECIES over P-256, an adversary that records encrypted sequencer traffic today may be able to decrypt it later once a cryptographically relevant quantum computer exists. This is harvest-now-decrypt-later risk. It is uniquely serious for Canton because the asset being protected is not only account control. It is institutional transaction privacy, counterparty privacy, position privacy, and settlement confidentiality. Historical encrypted data cannot be re-encrypted after an adversary has already collected it. Future migration does not erase past capture.

What should a Canton participant do about post-quantum privacy risk?

A Canton participant should first define the confidentiality horizon of its settlement data. If transaction views, counterparties, positions, or workflows must remain confidential for many years, harvest-now-decrypt-later exposure is a board-level issue, not a future technical task. The participant should inventory encryption schemes, key lifetimes, synchronizer exposure, archive-retention policy, custodian access, and vendor migration plans. It should separate historical data risk from future issuance risk. Historical ECIES-encrypted traffic may remain exposed even if future Canton versions add PQC. For new long-duration issuance or settlement workflows, institutions should evaluate PQ-native infrastructure where signing and privacy assumptions are designed for post-quantum security from inception.

Can MPC custody make ECDSA or Ed25519 assets post-quantum safe?

No. MPC changes key management, not the underlying signature scheme. An MPC wallet can split control of an ECDSA or Ed25519 private key across multiple parties, reducing single-point custody risk under classical assumptions. But if the final onchain signature is ECDSA or Ed25519, the asset still depends on a quantum-vulnerable public-key scheme. Once a cryptographically relevant quantum computer can recover private keys from exposed public keys, distributing the key shares does not make the signature algorithm quantum safe. MPC is valuable custody infrastructure. It is not a substitute for post-quantum signatures, post-quantum address design, and post-quantum verification logic.

Is Fireblocks quantum safe?

Fireblocks is a leading institutional custody and wallet infrastructure provider, but the assets and flows it supports can still rely on ECDSA, Ed25519, ERC-2612 permit, EIP-712 signing, and ERC-3643 ONCHAINID verification. Fireblocks MPC protects key operations, but MPC does not change the cryptographic assumptions of the chain or token standard. If the final signature is ECDSA or Ed25519, the signature remains quantum-vulnerable. If a custody policy approves Permit2 or ERC-2612 flows, the approval layer still depends on ECDSA verification. The institutional question is therefore not whether Fireblocks is operationally strong. It is whether the asset, chain, and standard being custodied are post-quantum safe.

Is BlackRock BUIDL quantum vulnerable?

Yes, at the infrastructure layer. BUIDL itself uses clean-port token standards such as ERC-20 and ERC-4626, which are not the core problem. The exposure comes from the surrounding Ethereum stack: secp256k1 address assumptions, active wallet public-key exposure, custody signing flows, ECDSA approvals, DeFi routing through immutable contracts, and potential permit or approval integrations. If BUIDL or similar tokenized funds interact with liquidity, custody, transfer agency, or settlement infrastructure that depends on ECDSA, the product inherits post-quantum risk. This is the broader lesson for tokenized funds: clean token interfaces are not enough if the operating rail remains quantum-vulnerable.

How does quantum computing threaten DeFi and institutional tokenization?

Quantum computing threatens DeFi and institutional tokenization through the same root issue: elliptic-curve public-key cryptography. Ethereum uses secp256k1 ECDSA, Solana uses Ed25519, and Canton uses Ed25519, ECDSA curves, and ECIES P-256 encryption. DeFi and institutional products are not separate stacks. Tokenized funds use DeFi liquidity, custody platforms approve DeFi transactions, stablecoins route through permit and approval systems, and regulated securities depend on identity and transfer restrictions. When the shared cryptographic base fails, the institutional layer fails with it. The report's central point is that there is no firewall between institutional tokenization and the crypto infrastructure it uses.

What is a Cryptographic Bill of Materials, or CBOM, for blockchain products?

A Cryptographic Bill of Materials is an inventory of the cryptographic algorithms, libraries, keys, and dependencies used by a system. For blockchain products, a CBOM cannot stop at the issuer's backend. It must include the underlying chain, signature algorithm, address derivation method, precompiles, smart-contract standards, identity systems, custody signing flows, wallet integrations, hardware security modules, MPC providers, encrypted settlement data, and immutable contracts. A tokenized product that says it is institution-grade but cannot name its ECDSA, Ed25519, ECIES, permit, and ONCHAINID dependencies is not ready for serious post-quantum diligence.

What are the estimated post-quantum TPS losses on Ethereum, Solana, and Canton?

The report treats throughput impact as a modeled migration problem, not a claim that every chain has already published confirmed numbers. Direct substitution of large PQ signatures into chains designed for compact ECDSA or Ed25519 signatures can create severe bandwidth, block-size, verification, and consensus overhead. SPHINCS+ signatures are far larger than classical signatures, and naïve migration can therefore reduce effective throughput materially. The exact loss depends on scheme choice, batching, aggregation, verifier design, transaction format, networking, and consensus architecture. The institutional conclusion is stable even if precise numbers change: existing chains were not designed around PQ signature sizes from genesis. PQ-native systems can design around those constraints before liquidity, custody, and settlement dependencies become immovable.

What is a PQ-native blockchain?

A PQ-native blockchain is infrastructure designed around post-quantum cryptography from genesis, not a classical chain trying to retrofit PQ later. It uses post-quantum signature assumptions for accounts, transaction authorization, verifier logic, and system design from the start. It avoids legacy ECDSA or Ed25519 address debt, frozen permit interfaces, immutable classical verifier contracts, and historical privacy systems based on quantum-vulnerable elliptic curves. The point is not simply adding one PQ algorithm. The point is removing inherited cryptographic debt across the full stack: keys, addresses, signatures, contracts, standards, custody flows, settlement privacy, and governance dependencies.

Why is PQ-native infrastructure safer than migrating Ethereum, Solana, or Canton later?

PQ-native infrastructure is safer because it avoids the hardest problem: coordinated migration of already-deployed economic systems. Ethereum must contend with immutable contracts, frozen ABIs, exposed public keys, L2 dependencies, wallets, and DeFi integrations. Solana must contend with Ed25519 authority keys, SPL Token immutability, GPU pipeline rewrites, validator and vote keys, and program upgrade authorities. Canton must contend with namespace identity permanently bound to classical keys, Synchronizer-enforced scheme gates requiring simultaneous institutional migration, KMS provider constraints, six-layer signing dependencies, and irreversible HNDL privacy exposure on $60T+ in historical settlements. A PQ-native chain starts without those liabilities. It begins with the target security model instead of trying to repair the old one.

Why does EternaX solve this structurally rather than as a patch?

EternaX is positioned as PQ-native institutional market infrastructure, not a patch layer on top of legacy cryptography. The structural difference is that EternaX is designed so the chain, account model, signature assumptions, verifier logic, and institutional application standards can be built for post-quantum requirements from genesis. It does not depend on converting old ECDSA addresses, replacing immutable Permit2 deployments, forcing ERC-2612 to accept signatures it cannot encode, re-authorizing SPL Token, or trying to erase historical ECIES privacy debt. That is why EternaX is the natural architectural conclusion of the report: institutions do not need to repair Ethereum, Solana, or Canton. They need rails that do not require repair.

Can tokenized funds continue using Ethereum while becoming fully post-quantum safe?

Only partially. Some standards, including ERC-20, ERC-721, ERC-4626, ERC-4337, and newer signature-agnostic standards, can be ported or adapted more cleanly. But full post-quantum safety requires more than a clean token interface. It requires PQ-safe wallets, PQ-safe custody flows, PQ-safe admin controls, PQ-safe permit or approval mechanisms, PQ-safe identity and compliance logic, and avoidance of immutable classical contracts. A tokenized fund can reduce exposure on Ethereum, but it cannot make the full legacy environment disappear. For new issuance, the cleaner strategic choice is to separate future institutional products from avoidable cryptographic debt.

Which standards are not the main problem and why does this report exclude them?

The report intentionally excludes clean-port standards that are not structurally broken by hardcoded ECDSA or Ed25519 verification. ERC-20, ERC-721, ERC-4626, ERC-4337, and ERC-7943 are not the central issue because they can be redeployed or adapted on PQ-native rails without the same frozen-signature problem. The report focuses on what cannot be fixed in place: ERC-3643 ONCHAINID ECDSA claim verification, ERC-2612 v/r/s permit, ERC-1400 certificate controllers, ecrecover dependencies, immutable contracts, SPL Token authority logic, Solana runtime primitives, and Canton ECIES privacy. This improves credibility because it avoids claiming everything is broken. It focuses only on the parts that create non-upgradeable institutional risk.

What should institutional issuers, custodians, and settlement participants do now?

Institutions should stop treating post-quantum migration as a protocol-team problem. The immediate task is a cryptographic exposure map: identify every chain, signature scheme, address model, smart-contract standard, permit flow, custody provider, MPC or HSM dependency, compliance verifier, immutable contract, and encrypted settlement path used by the product. Then classify each dependency as clean-port, replaceable, coordination-heavy, or non-upgradeable. Existing products may need containment and migration planning. New products should avoid fresh issuance on rails with known non-upgradeable cryptographic debt. The strategic conclusion is simple: choose infrastructure where post-quantum security is native to the architecture, not an unresolved future retrofit.

Founding Team

10+ Years at the Intersection of Blockchain Infrastructure, Institutional Finance, and Post-Quantum Cryptography

The team behind EternaX combines protocol research, cryptography, distributed systems, institutional digital-assets strategy, and post-quantum market-infrastructure execution.

Dariia Porechna

CO-FOUNDER

Cryptographer and distributed systems architect; Head of Protocol, Subspace; Research Engineer, Wolfram|Alpha. Co-author, SILMARILS.

LINKEDIN X

Paarrthhh Birla

CO-FOUNDER

Ex-Polygon (VP Growth Office); Head of Partnerships, Subspace Protocol; digital-assets strategy at EYP, advised Visa and State Street; MBA, CPA.

LINKEDIN X

Dr. Chen Feng

CHIEF SCIENTIST

Associate Professor at University of British Columbia; PhD, University of Toronto; 100+ peer-reviewed papers; quantum communications, blockchain, and TEE privacy. Co-author, SILMARILS.

LINKEDIN SCHOLAR

Contact

Institutional Inquiries

For institutional inquiries regarding post-quantum financial infrastructure, tokenization post-quantum risk, custody post-quantum exposure, cryptographic migration debt, EO 14412 compliance, or EternaX PQ-native infrastructure.

Paarrthhh Birla - Co-Founder - paarrthhh.b@eternax.ai

Dariia Porechna - Co-Founder - dariia.p@eternax.ai

SCOPE, METHODOLOGY, AND LIMITATIONS

This report maps institutional post-quantum exposure across Ethereum, Solana, and Canton. It focuses on non-upgradeable cryptographic dependencies in immutable contracts, frozen standards, exposed public keys, identity systems, custody workflows, and historical encrypted settlement data. Claims are anchored to primary standards and protocol documentation as of July 2026. Institution-specific exposure and dollar figures should be refreshed against live product disclosures before each publication cycle. This report does not constitute investment, legal, or regulatory advice.

Authors: Paarrthhh Birla, Dr. Chen Feng, Dariia Porechna · EternaX Labs · Published July 1, 2026

Citation: EternaX Labs, "Your Chain Will Not Save You: Post-Quantum Institutional Risk Across Ethereum, Solana, and Canton," July 2026. eternax.ai