ETERNAX RESEARCH · INSTITUTIONAL POST-QUANTUM FRAMEWORK · APRIL 2026

Cryptographic Migration Debt:
The Post-Quantum Exposure Framework for Institutional Digital Asset Programmes

Why BlackRock, JPMorgan, Franklin Templeton, Visa, DTCC, and Fidelity are building at scale on rails that will require expensive, privacy-fragile, vendor-dependent migration for assets that never needed to carry that liability — and what institutions must do before issuing another dollar of long-duration value on-chain.

PUBLISHED
APRIL 2026

AUTHORS
PAARRTHHH BIRLA, CO-FOUNDER · DR. CHEN FENG, CHIEF SCIENTIST · DARIIA PORECHNA, CO-FOUNDER

AUDIENCE
BOARDS · RISK COMMITTEES · TOKENIZATION TEAMS · STABLECOIN ISSUERS · CUSTODIANS · ENTERPRISE DIGITAL ASSET PROGRAMMES

Not investment advice. EternaX novel PQ scheme pending IACR Journal of Cryptology publication. Sections 1–14 present independent analysis sourced from public records, federal standards, peer-reviewed research, and published statements. EternaX architecture and positioning are presented in Section 15. All market data as of April 2026.

SIX FACTS EVERY BOARD, RISK COMMITTEE, AND INSTITUTIONAL DIGITAL ASSET TEAM MUST ACT ON IN 2026

$200B

In stablecoins and tokenized RWAs on Ethereum governed by admin keys Google has identified as quantum-vulnerable. This is the institutional control-surface number, not the wallet number.

90%

Throughput loss on Solana in live testnet using quantum-resistant signatures — confirmed April 2026 by Project Eleven and the Solana Foundation. Quantum-safe Solana today is not commercially viable.

0

End-to-end post-quantum roadmaps disclosed by any of the named institutional programmes — BlackRock BUIDL, JPMorgan MONY, Franklin FOBXX, WisdomTree, Visa, DTCC, Fidelity FYOXX, Fidelity FIDD (launched Feb 2026), major stablecoin issuers.

20×

Reduction in the qubit threshold for breaking Bitcoin and Ethereum's cryptography. Google's March 2026 paper cut the requirement from ~9M to <500K physical qubits in a single publication.

$0

The cost of migration debt on the day of new PQ-native issuance. Compared to the coordination, legal, liquidity, and reputation cost of migrating an established programme later. New issuance is a choice.

4 yrs

"This is a tomorrow problem — until it's today's problem. And then it takes four years to fix." — Alex Pruden, CEO Project Eleven, April 4, 2026. The time to act is now, not at Q-day.

IF YOU HAVE 7 MINUTES — READ THIS BEFORE YOUR NEXT RISK COMMITTEE OR TOKENIZATION STRATEGY MEETING

Five arguments every board member, CRO, and tokenization team must understand before the next issuance decision

01 · THE INSTITUTIONAL SCALE IS ALREADY LIVE — AND GROWING

BlackRock's BUIDL fund holds **$2.85 billion** across nine public blockchains. JPMorgan launched a tokenized money market fund on Ethereum in December 2025. Visa settles **$3.5 billion annualized** in stablecoin via Solana. DTCC is tokenizing U.S. Treasuries on approved public blockchains from H2 2026. Fidelity launched **FIDD** — a new institutional stablecoin on Ethereum mainnet — in February 2026. Not one of these programmes has a disclosed end-to-end post-quantum cryptographic roadmap. The exposure is live, operational, and growing every quarter.

02 · GOOGLE COMPRESSED THE TIMELINE 20× IN A SINGLE PAPER

On March 30, 2026, Google Quantum AI published a whitepaper showing that breaking Bitcoin and Ethereum's cryptography requires roughly **500,000 physical qubits** — down from ~9 million. Same day, Oratomic/Caltech showed the same attack possible with as few as **9,739 qubits** in under three years. Google called this *"a singular discontinuity in the history of digital security."* The "we have decades" heuristic is no longer defensible enterprise posture.

03 · THE INSTITUTIONAL RISK IS THE CONTROL PLANE, NOT THE WALLET

Google estimates **$200 billion** in stablecoins and tokenized RWAs on Ethereum depends on admin keys already exposed on-chain — crackable in under 15 hours on a fast-clock quantum machine. The April 1, 2026 **$285 million** Drift exploit showed what reaching a Security Council costs today: 3 weeks of social engineering. Under quantum threat, that social engineering step is eliminated for exposed key surfaces.

04 · THE BOARD QUESTION IS NOT "WHEN" — IT IS "WHY"

Stablecoins, tokenized treasuries, and most RWAs derive value from **off-chain reserves, legal claims, and sovereign credit**. Those assets should not be contaminated by avoidable cryptographic migration debt from the wrong blockchain rail. The right question is not when will quantum computers arrive. It is: why are we **still issuing long-duration value** onto rails that guarantee an avoidable future liability for assets that never needed to carry it?

05 · ON-CHAIN PRIVACY IS NOT PERMANENT — AND NEITHER IS YOUR CONFIDENTIALITY

State actors are **already collecting blockchain data** to decrypt later. Every treasury movement, counterparty relationship, settlement flow, and investor identity recorded on a public rail today is being archived for retroactive decryption once quantum capabilities mature. The harvest-now-decrypt-later threat does not wait for Q-Day — it accumulates silently as the permanent on-chain record grows. Institutions moving to on-chain finance need privacy that **stays private under quantum threat**, not privacy that expires. And they need selective disclosure for compliance — simultaneously, not traded off against each other. That architecture exists. It is not Ethereum. It is not Zcash. It is not Monero. And it is not Circle's Arc as currently designed.

CONTENTS

BlackRock's BUIDL fund holds **$2.85 billion** across nine public blockchains. JPMorgan Asset Management launched its first tokenized money market fund on Ethereum in December 2025. Franklin Templeton's on-chain U.S. Government Money Fund operates across nine approved public networks. Visa settled over $3.5 billion in annualized stablecoin volume through partner banks over Solana. DTCC received an SEC no-action letter to tokenize DTC-custodied securities on approved public blockchains from H2 2026. Fidelity launched the Fidelity Digital Dollar (FIDD) — a new institutional stablecoin issued by Fidelity Digital Assets, NA on Ethereum mainnet — in February 2026. Fidelity FYOXX, its tokenized money market fund, has been live on Ethereum since mid-2025.

Not one of these programmes has a disclosed end-to-end post-quantum cryptographic roadmap covering custody, admin controls, settlement mechanics, interoperability, and audit.

That gap is the problem this report addresses. Post-quantum risk to stablecoins and tokenized RWAs is not primarily about wallets being stolen. It is about **migration debt** accumulating from the moment of issuance. **Control-plane vulnerability** concentrating institutional exposure in admin key surfaces that are permanently exposed on-chain. **Privacy degrading retroactively** for on-chain transaction data already recorded — meaning today's transactions are tomorrow's intelligence for an adversary with a quantum computer. And **blockchain rail risk contaminating** off-chain assets with cryptographic liabilities they never needed to carry. The question is not whether to tokenize. It is which rails the next generation of institutional value should be issued on — and what happens to the assets already on the wrong ones.

IF YOU ARE INVOLVED IN DIGITAL ASSETS, TOKENIZATION, CUSTODY, SETTLEMENT, OR ON-CHAIN FINANCE — THIS REPORT IS ABOUT YOU

Find Yourself. Find Your Risk. Find Your Next Step.

IF YOU ARE…	YOUR PRIMARY PQ EXPOSURE	YOUR BIGGEST CONTROL-PLANE RISK	YOUR PRIVACY RISK	WHAT TO DO NOW
Stablecoin issuer USDC, FIDD, PYUSD, Tether, USDT	Rail + admin keys governing mint/burn/freeze authority over the full circulating supply	A quantum attacker forging a mint transaction creates unlimited token supply decoupled from reserves	Treasury movements, reserve rebalancing, and redemption patterns permanently on-chain	**Stop new issuance on vulnerable rails. Map mint/burn/freeze key exposure. Engage custodian on PQ roadmap now.**
Tokenized fund / RWA manager BUIDL, MONY, FOBXX, FYOXX	Rail + transfer-agent logic + bridge dependencies across every chain the fund operates on	Admin and upgrade keys governing fund contract logic — if forged, can redirect investor redemptions or destroy NAV accounting	Investor wallet identities, fund flows, and counterparty relationships observable on public rails	**Freeze further chain expansion. Map all transfer-agent and bridge dependencies. Block new fund launches on legacy rails.**
Custodian BitGo, Fidelity Digital Assets, Anchorage, Coinbase Custody	Key management perimeter — HSMs, cold/warm signing infrastructure, policy-engine authorization chains	Master custody keys and omnibus signing controls; if exposed, the attacker controls all client assets simultaneously	Client flow intelligence, asset positions, and transaction patterns visible through custody layer	**Inventory all signing keys and their on-chain exposure. Require PQ roadmap from every key-management vendor. Begin rotation planning.**
Exchange / prime broker Coinbase, Binance, OKX, Bybit, Hyperliquid	Settlement and omnibus wallet exposure; hot-wallet signing perimeters; withdrawal authorization chains	Hot-wallet governance and treasury keys; a quantum attack on exposed omnibus keys drains all depositor funds without social engineering	Position sizes, trading intent, counterparty flow patterns permanently observable	**Inventory all exposed control keys across hot, warm, and settlement layers. Require PQ attestation from counterparty custodians.**
Tokenization platform Securitize, Fireblocks, Tokeny, Apex	Issuance and approval workflows — your platform's admin keys govern the compliance and ownership state of every asset issued through you	Transfer-agent and admin logic; a platform with exposed upgrade keys loses ownership of the entire issuance compliance model	Investor KYC linkages, ownership records, and transfer approval histories — a permanent on-chain intelligence archive	**Publish a PQ roadmap or disclose the absence of one to all clients. A platform with no roadmap is creating liability for every issuer who depends on it.**
Oracle / bridge / attestation Chainlink, Wormhole, CCTP, LayerZero	Signer perimeter — oracle and bridge attesters are among the highest-value at-rest targets in the entire ecosystem	A forged bridge attestation can drain the entire locked-value reserve of a bridge; Wormhole exploit was $320M via guardian key compromise	Routing decisions, cross-chain flow patterns, and price-feed dependencies permanently observable	**Treat signer migration as top priority. Map every attester key's on-chain exposure. Bridge and oracle PQ migration cannot wait for chain upgrades.**

IF YOU ARE…	YOUR PRIMARY PQ EXPOSURE	YOUR BIGGEST CONTROL-PLANE RISK	YOUR PRIVACY RISK	WHAT TO DO NOW
Bank / payment processor Visa, JPMorgan, DTCC, Stripe/Bridge	Settlement and treasury integration points where traditional finance connects to on-chain rails — each connection point inherits rail-level PQ risk	Internal approval keys and custody controls for stablecoin and tokenized-settlement flows; if on-chain, they are permanently exposed	Treasury and counterparty flow data; strategic payment routing and settlement patterns visible on public rails	**Separate legacy on-chain settlement exposure from future issuance decisions. Require PQ roadmap from every blockchain rail used for institutional settlement.**

THIS REPORT DIRECTLY ANSWERS

- → What is the quantum threat to crypto?
- → What is post-quantum risk to stablecoins and tokenized RWAs?
- → What is migration debt in blockchain?
- → What is control-plane vulnerability in crypto?
- → What is post-quantum risk in Ethereum, Solana, and Bitcoin?
- → What is PQ-safe auditable privacy?
- → What is harvest-now-decrypt-later risk?
- → What should institutions do before new on-chain issuance?
- → What is PQ-native issuance?
- → Why is Fidelity FIDD a post-quantum risk case study?

EXECUTIVE SUMMARY

Five Claims and the Central Thesis

GOOGLE QUANTUM AI · MARCH 30, 2026 · CO-AUTHORED WITH ETHEREUM FOUNDATION & STANFORD · 57 PAGES · ZERO-KNOWLEDGE PROOF OF RESOURCE ESTIMATES

"The expected emergence of cryptographically relevant quantum computers will represent a singular discontinuity in the history of digital security, with wide ranging impacts."

— "Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations" · Ryan Babbush, Craig Gidney, Hartmut Neven et al. (Google Quantum AI), Justin Drake (Ethereum Foundation), Dan Boneh (Stanford)

SUMMARY

Google's March 30, 2026 whitepaper lowered the physical qubit threshold for breaking secp256k1 by approximately twenty-fold — from prior estimates of ~9 million to fewer than 500,000. On-spend attacks on live blockchain transactions are feasible within Bitcoin's ten-minute block window on fast-clock architectures. Google extended the problem explicitly to Ethereum's smart contracts, stablecoins, tokenized real-world assets, Proof-of-Stake validators, Layer 2 networks, and privacy-preserving systems. The same day, Oratomic and Caltech published a preprint showing Shor's algorithm executes for ECC-256 with as few as 9,739 atomic

qubits in under three years. Google's paper included Section VI.D — "Stablecoins and Real-World Asset Tokenization" — the first tier-one technical institution to formally publish a vulnerability taxonomy for institutional-scale on-chain finance.

This report makes five claims. **First,** the most important enterprise consequences arrive before any theft — through migration debt, control-plane fragility, privacy contamination, vendor dependence, and market-structure repricing that can begin before any public cryptographic break. **Second,** the correct unit of analysis is the enterprise workflow, not the chain in isolation. **Third,** legacy exposure and new issuance are different decisions. **Fourth,** privacy is a first-class institutional requirement that must rest on information-theoretic or post-quantum cryptographic foundations to be durable over long time horizons. **Fifth,** a credible destination architecture must solve the full stack simultaneously — PQ-safe authorization, migration support, custody and policy integration, auditable privacy, and commercial execution quality.

CENTRAL THESIS

Assets whose value derives from outside the blockchain — stablecoins, tokenized treasuries, tokenized deposits, money market funds, and most RWAs — should not be contaminated by avoidable blockchain-native cryptographic debt, control-plane fragility, and privacy degradation simply because the wrong rail was chosen at issuance. The blockchain is the rail. It is not the source of value. Rails should not impose permanent liabilities on the assets they carry.

HOW TO READ THIS REPORT — EVIDENCE STANDARDS	
Confirmed fact	Explicitly stated in a named primary source: Google Quantum AI whitepaper, Project Eleven live testnet, NIST FIPS, Ethereum Foundation pq.ethereum.org, named institutional press releases.
Architecture inference	Derived from confirmed public facts about system design — e.g., Ethereum permanently exposes public keys on first transaction is an architectural property, not a speculative claim.
Open diligence item	Cannot be confirmed from the public record. Institutional diligence required. Labelled as "Requires Diligence" where it appears in rubric tables.
Disclosed PQ roadmap standard	To qualify as "disclosed" in this report, a roadmap must be: publicly available, time-bound, and cover the full workflow — including custody, admin control surfaces, settlement mechanics, interoperability, and privacy. "The chain may upgrade later" does not qualify.
Not sufficient	"We are monitoring the quantum threat." "We will migrate when the chain does." "Our chain has a PQ roadmap." — None of these satisfy the end-to-end disclosure standard used in this report.

REFERENCE DATA

The Numbers That Change the Conversation

<500K

PHYSICAL QUBITS TO BREAK SECP256K1 (GOOGLE, MAR 30 2026). ~20× REDUCTION FROM PRIOR ~9M ESTIMATE. MINUTES OF EXECUTION ON SUPERCONDUCTING ARCHITECTURE. THE TIMELINE JUST COMPRESSED BY 20×.

9,739

MINIMUM ATOMIC QUBITS (ORATOMIC/CALTECH) FOR ECC-256. UNDER 3YR RUNTIME. 26,000 QUBITS: ~10 DAYS. MANUEL ENDRES HAS ALREADY TRAPPED 6,000 ATOMIC QUBITS. THE HARDWARE TRAJECTORY IS CONCRETE.

~9 min

ON-SPEND ATTACK WINDOW AGAINST BITCOIN (41% SUCCESS PROBABILITY WITHIN 10-MIN BLOCK TIME). SOLANA'S ~400MS FINALITY SIGNIFICANTLY NARROWS THIS FOR ON-SPEND ATTACKS SPECIFICALLY.

$200B

GOOGLE ESTIMATE: STABLECOINS AND TOKENIZED RWAS ON ETHEREUM DEPENDENT ON ADMIN-VULNERABLE KEYS. THE INSTITUTIONAL CONTROL-SURFACE NUMBER, NOT THE USER-WALLET NUMBER.

2.5M ETH

IN AT LEAST 70 ADMIN-VULNERABLE CONTRACTS (TOP 500 BY ETH BALANCE). CRACKABLE IN <15 HOURS ON FAST-CLOCK CRQC — WITHOUT SOCIAL ENGINEERING A SINGLE PERSON.

37M ETH

STAKED ETH SECURED BY BLS SIGNATURES GOOGLE CONSIDERS QUANTUM-VULNERABLE. LIDO ALONE HOLDS ~20%, CONCENTRATING CONSENSUS-LAYER ATTACK SURFACE.

15M ETH

ACROSS MAJOR L2S AND CROSS-CHAIN BRIDGES. EACH MUST UPGRADE INDEPENDENTLY — A BASE-LAYER FIX COVERS NONE OF THIS EXPOSURE.

$317B+

TOTAL STABLECOIN MARKET CAP, EARLY 2026. $33 TRILLION IN STABLECOIN TRANSACTION VOLUME IN 2025. ALL ON QUANTUM-VULNERABLE RAILS WITH NO DISCLOSED MIGRATION ROADMAP.

$36B+

TOKENIZED RWAS (EX-STABLECOINS) ON-CHAIN AS OF LATE 2025, UP 300%+ IN 18 MONTHS. ETHEREUM HOLDS ~65%. INSTITUTIONS ARE LOCKING IN RAIL CHOICES FASTER THAN MIGRATION PLANS.

2029

ETHEREUM FOUNDATION'S TARGET FOR BASE-LAYER PQ UPGRADE. THEIR EXPLICIT STATEMENT: "FULL EXECUTION-LAYER MIGRATION TAKING ADDITIONAL YEARS BEYOND THAT." DOES NOT COVER DEPLOYED CONTRACTS.

$285M

DRIFT PROTOCOL EXPLOIT, APRIL 1, 2026. REACHED SECURITY COUNCIL VIA 3-WEEK SOCIAL ENGINEERING. UNDER QUANTUM THREAT, THAT STEP IS ELIMINATED FOR EXPOSED KEY SURFACES.

0

NAMED INSTITUTIONAL PROGRAMMES — BUIDL, FOBXX, MONY, FYOXX, VISA STABLECOIN SETTLEMENT, DTCC TOKENIZATION, WISDOMTREE — WITH DISCLOSED END-TO-END POST-QUANTUM ROADMAPS.

Sources: Google Quantum AI whitepaper (March 30, 2026); Oratomic/Caltech arXiv:2603.28627 (March 30, 2026); Ethereum Foundation pq.ethereum.org (March 24, 2026); DTCC/SEC no-action letter (December 11, 2025); NIST FIPS 203/204/205 (August 2024); BlackRock/Securitize, JPMorgan AM, Franklin Templeton, Visa, Fidelity, WisdomTree primary press releases; Elliptic/TRM Labs (Drift, April 2026).

SECTION 01

Post-Quantum Risk Before Theft: *Migration Debt, Control-Plane Fragility, and the Market-Structure Repricing Argument*

The market is asking the wrong question. "When will wallets be cracked?" skips the enterprise consequences that arrive first and cost more. The most damaging institutional exposures under a compressing quantum timeline are not theft. They are the operational and financial liabilities that begin accruing the moment an asset is issued on the wrong rail.

TABLE 1.1 — ENTERPRISE CONSEQUENCES THAT ARRIVE BEFORE ANY PUBLIC THEFT EVENT

CONSEQUENCE	WHAT IT MEANS IN PRACTICE	WHY IT MATTERS BEFORE ANY PUBLIC BREAK
Rail-induced asset contamination	Assets issued on non-PQ-safe rails absorb a market risk premium that their underlying credit, legal structure, or reserve quality would otherwise not justify	A stablecoin backed 1:1 by dollars should not trade at a rail-induced discount. A tokenized Treasury fund should not absorb blockchain cryptographic risk. This is the central financial argument — and it begins before any attack occurs.
Migration debt	Future cost of re-platforming issuance, wallets, custody, exchange support, and compliance across every product on quantum-vulnerable rails	Accrues at issuance time, not at break time. Every new asset issued on a weak rail compounds the debt.
Control-plane fragility	Admin keys, mint/burn/freeze authority, governance multisigs, transfer-agent signing, bridge attesters concentrate institutional value that are more directly attackable than dispersed user wallets	For enterprises, the governance layer is more exposed than individual end-user accounts. A quantum computer targeting the admin key governing $200B in stablecoins does not need to attack a single wallet.
Privacy contamination	Balances, counterparties, flow timing, treasury movements on public rails carry permanent retroactive exposure risk as quantum capabilities improve	On-chain data is permanent. The cryptographic assumptions protecting it are not. Historical transaction data remains vulnerable to future decryption.
Vendor dependence	Tokenization providers, custodians, exchanges, and middleware may have no credible PQ roadmap — the institution's migration is governed by its slowest supplier	"The chain will upgrade later" does not fix supplier risk. The chain upgrading does not automatically migrate the supplier's signing perimeter.
Liquidity fragmentation	During migration, assets bifurcate into old and new forms across venues, custodians, and DeFi protocols	Pricing divergence, capital inefficiency, and compliance complexity arrive before the first key is attacked
Governance and board burden	Risk committees, boards, and regulators can ask today whether continued issuance on documented vulnerable rails is consistent with fiduciary standards given NIST finalization and Google's March 2026 paper	The governance freeze can arrive before any cryptographic failure

The market-structure repricing argument. Four mechanisms can trigger repricing without any CRQC existing. First, boards can ask now whether fiduciary duty requires addressing documented vulnerabilities against NIST-finalized standards. Second, auditors can advise now that continued issuance on documented vulnerable rails creates a disclosure

obligation to investors. Third, regulators monitoring stablecoin infrastructure can require quantum-exposure disclosures as part of reserve reporting. Fourth, institutional counterparties can begin applying risk haircuts to assets issued on rails with no disclosed PQ roadmap when pricing collateral or repo agreements. None require a quantum computer — they require only that institutional awareness reaches the same level as the public technical record. Google's paper, covered by Bloomberg, CoinDesk, and the Financial Times within hours of publication, has accelerated that process by years.

CONCRETE REPRICING MECHANISM — HOW A RAIL-INDUCED HAIRCUT FORMS

The scenario: It is Q3 2026. A repo desk at a major prime broker is pricing a bilateral repo against a tokenized U.S. Treasury MMF — say, a BUIDL-equivalent instrument with $2.85 billion in underlying Treasury securities, issued on Ethereum. The underlying credit is unimpeachable: U.S. government obligations in BNY custody. Standard repo haircut: 2%.

The repricing trigger: The prime broker's risk committee has read Google's March 2026 paper. They note that the fund's admin keys — which govern its upgrade authority, mint/burn mechanics, and transfer-agent logic — are permanently exposed on-chain and carry no disclosed PQ migration timeline. The committee adds a "cryptographic infrastructure risk" adjustment of 50–150 basis points to the repo haircut, citing undisclosed quantum-migration liability. The fund's sponsor cannot point to a credible PQ roadmap. The adjustment stands.

The structural implication: The underlying asset — U.S. Treasury securities — has not changed. The legal structure has not changed. The reserve quality has not changed. The haircut has changed because of the rail. The blockchain rail has imported a cryptographic liability into an instrument that, in its traditional form, carries none. This is not a theoretical mechanism. It is a standard risk-adjustment process applied to a newly identified risk factor that is now in the public record. The only question is when prime brokers, repo desks, and collateral managers begin applying it systematically.

> *"Migration debt starts accruing at issuance time, not at break time. Market-structure repricing can begin before any public break. Both facts mean this is already a present financial problem — not a future security problem."*

SECTION 02

The Quantum Threat to Crypto Is Not Distant: *Why CRQC Timeline Compression Changes the Institutional Calculus*

On March 30, 2026, Google compressed the qubit threshold for breaking Bitcoin and Ethereum's cryptography by twenty-fold in a single paper. Prior best estimate: ~9 million physical qubits. New estimate: fewer than 500,000 — running in minutes on standard superconducting architecture. Researchers validated their resource estimates using a zero-knowledge proof to avoid disclosing attack circuits — responsible disclosure at the scale of a national security implication. The same day, Oratomic and Caltech published independently showing the same attack executes with as few as 9,739 atomic qubits in under three years. Two independent research groups. Same conclusion. One day.

> *"It is conceivable that the existence of early cryptographically relevant quantum computers may first be detected on the blockchain rather than announced."*
>
> — Google Quantum AI Whitepaper, March 30, 2026

Oratomic co-founder Manuel Endres has already trapped arrays of 6,000 atomic qubits — hardware trajectory is concrete, not theoretical. Their paper shows ECC-256 attacks execute with 9,739 qubits in under three years, 11,961 qubits in under one year, and ~26,000 qubits in approximately ten days.

> *"It is plausible, although not guaranteed, that we will have a fault-tolerant quantum computer by the end of the decade."*
>
> — Dolev Bluvstein, CEO, Oratomic (Caltech spin-out), March 31, 2026

> *"My confidence in a Q-day by 2032 has risen sharply. I now see at least a 10% chance that a quantum computer could recover a secp256k1 private key within six years."*
>
> — Justin Drake, Ethereum Foundation researcher and co-author of Google quantum whitepaper, March 2026

> *"Elliptic curve cryptography is on the brink of obsolescence. Whether it's 3 or 10 years, it's over and we need to accept that."*
>
> — Nic Carter, Co-Founder, Castle Island Ventures, Bankless Podcast, April 2026

> *"We're in the equivalent of 1940 — since the Google Willow result we've known this was theoretically possible. There were no new physics discoveries that needed to occur. Now we're at the point where we just have to do the engineering."*
>
> — Nic Carter, Co-Founder, Castle Island Ventures, Bankless Podcast, April 2026

The Manhattan Project analogy is precise in a way that matters institutionally. The atomic bomb went from theoretical proof of fission (1938) to Trinity test (1945) in seven years, once the engineering began. The engineering on quantum computing began in earnest with Google's Willow processor in late 2024. The seven-year clock, if the analogy holds, runs to 2031. That is not a distant horizon. It is inside the asset-life window of every institutional digital asset programme currently operating.

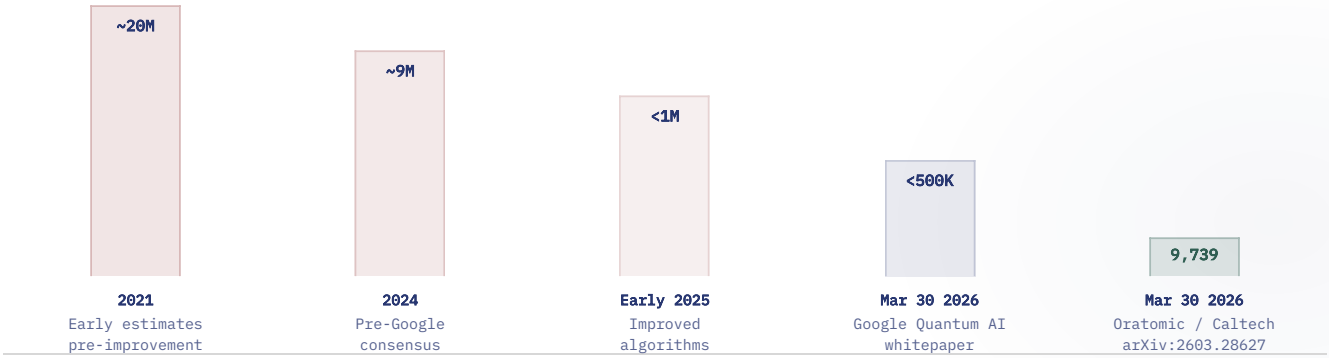
> *"The assumption inherent in what Sailor is saying is we will have a very clear notice period before Qday comes. But it's not like Y2K. Nobody knows the day or the hour. It will just happen one day."*
>
> — Nic Carter, Co-Founder, Castle Island Ventures, Bankless Podcast, April 2026

The no-notice-period argument is the most consequential element of both Google's paper and the analyst consensus it has generated. Google's own authors state explicitly that a threshold model is the correct planning assumption — meaning the transition from a non-threatening environment to a CRQC will be abrupt rather than gradual. Institutions that are banking on having 18–24 months of lead time from public announcements to plan and execute a migration are planning for a scenario the authors of the paper say will not occur.

Cloudflare has already completed its post-quantum migration. The internet infrastructure in use today by institutions communicating about these risks is already post-quantum. Apple, Google, and the US government have all set internal migration targets of 2029–2030. Google's Android 17 will ship ML-DSA post-quantum digital signature protection natively

— meaning the mobile operating system used by over three billion people will have PQ signatures by default before most blockchains have a migration plan. Every major institution on the planet is aware of and actively mitigating post-quantum risk. The institutional blockchain stack — carrying $317 billion in stablecoins and $36 billion in tokenized RWAs — is the outlier, not the standard.

THE QUBIT COMPRESSION TRAJECTORY — PHYSICAL QUBITS REQUIRED TO BREAK SECP256K1 / ECC-256



Direction of travel: Every year, the required qubit count falls. The 9,739 figure represents a ~2,000× compression from 2021 estimates. **Smaller bar = fewer qubits needed = more dangerous.** The direction has been consistent for a decade. Institutions that anchored on prior-year estimates have been wrong in the same direction every time. The comfortable planning window is structurally shrinking.

ATTACK TYPE 01

On-Spend Attack

Targets live mempool transactions before confirmation. Requires fast-clock CRQC. ~9 min window for Bitcoin (41% success probability within 10-min block time). Ethereum's ~12s finality narrows this. Solana's ~400ms finality provides strong structural protection against on-spend attacks specifically.

→ **Active transactions at risk on slow-finality chains**

ATTACK TYPE 02

At-Rest Attack

Targets permanently exposed public keys. No time pressure — days or more available. Both fast-clock and slow-clock CRQCs execute this. ~6.9M BTC in vulnerable addresses. Ethereum permanently exposes public keys on first transaction — no rotation without account abandonment. All exposed admin keys are at-rest targets.

→ **Every exposed admin key is a permanent, never-expiring target**

ATTACK TYPE 03

On-Setup Attack

One-time quantum computation recovers "toxic waste" from a cryptographic ceremony (Ethereum's KZG trusted setup for Data Availability Sampling), creating a permanent reusable classical backdoor. Bitcoin is immune. Ethereum's DAS mechanism is explicitly vulnerable. Requires CRQC only once — all subsequent exploits are classical.

→ **One CRQC computation permanently compromises all L2 infrastructure on Ethereum**

"Nobody knows the day or the hour. It will just happen one day. Google compressed the qubit buffer by 20× in a single paper, and their own authors say there will be no significant notice period before a CRQC exists. Institutions cannot plan for a warning that will not come."

SECTION 03

Post-Quantum Risk on Ethereum, Solana, and Bitcoin: *Why the Institutional Story Is the Stablecoin and Tokenized RWA Control Plane*

The public reaction to Google's paper focused almost entirely on Bitcoin. That reaction misses the institutional story. Google's paper includes a dedicated section — **Section VI.D, "Stablecoins and Real-World Asset Tokenization"** — that explicitly maps quantum vulnerabilities to the institutional tokenization ecosystem. It notes that financial developments "such as fiat-backed stablecoins and tokenization of other real-world assets, are projected to increase the pool of assets governed by smart contracts by nearly an order of magnitude by 2030." This is the first time a tier-one technical institution has formally catalogued these exposures in a peer-reviewed-pathway publication.

On Ethereum, five distinct vulnerability classes exist. **Account vulnerability:** Ethereum permanently exposes a user's public key on first transaction — top 1,000 wallets hold ~20.5 million ETH, all exposed, with no rotation mechanism without abandoning the account. **Admin vulnerability:** at least 70 of the top 500 contracts by ETH balance have admin keys on-chain, holding ~2.5 million ETH crackable in under 15 hours — and those keys govern ~$200 billion in stablecoins and tokenized assets. **Consensus vulnerability:** ~37 million ETH staked using BLS signatures Google considers quantum-vulnerable; Lido holds ~20%, concentrating attack surface. **L2 vulnerability:** at least 15 million ETH across rollups and bridges; each must upgrade independently. **Data availability vulnerability:** the KZG ceremony underpinning Ethereum's DAS creates a one-time-attack, permanently-exploitable classical backdoor.

TABLE 3.1 — ETHEREUM'S FIVE QUANTUM VULNERABILITY CLASSES

VULNERABILITY	SCALE	ATTACK TIME (FAST-CLOCK)	ETH 2029 ROADMAP COVERS THIS?
Account vulnerability	~20.5M ETH in top 1,000 wallets	<9 days for all 1,000 at 9 min/key	**Partially**
Admin vulnerability	~2.5M ETH in 70+ contracts; ~$200B stablecoins/RWAs governed by same keys	<15 hours per admin key	**No — contracts upgrade independently**
Consensus vulnerability	~37M ETH staked; Lido ~20% concentration	Pool concentration shortens timeline	**Partially (Fork I, 2026)**
L2 vulnerability	>15M ETH across major L2s/bridges	Depends on key exposure	**No (Fork M, post-2029)**
Data availability vulnerability	KZG setup: universal reusable backdoor	One-time CRQC → permanent classical exploit	**No (requires full DA redesign)**

POST-QUANTUM RISK ON BITCOIN — THE HIGHEST-TRAFFIC QUERY, ANSWERED PRECISELY

Post-quantum Bitcoin risk is the most-searched query in this space and deserves a precise, standalone answer. Bitcoin's primary quantum vulnerability is the at-rest attack against addresses whose public keys are permanently exposed on-chain. This exposure arises in three ways: Pay-to-Public-Key (P2PK) scripts from the Satoshi era (~1.7 million BTC, all with public keys permanently on-chain); address reuse across wallet types; and the Taproot upgrade (2021), which made public keys visible by default and expanded the vulnerable pool. Google estimates approximately 6.9 million BTC are currently in addresses with some form of public-key exposure — roughly one-third of total circulating supply.

Bitcoin is immune to on-setup attacks (no trusted cryptographic ceremonies) and its Proof-of-Work consensus mechanism is not vulnerable to Shor's algorithm. For on-spend attacks, Google modeled that a fast-clock superconducting CRQC could derive a secp256k1 private key in approximately nine minutes — close enough to Bitcoin's ten-minute average block time to create a ~41% theft probability on live mempool transactions. This is the "on-spend" window that generated most media coverage. Bitcoin has no disclosed end-to-end post-quantum migration plan as of April 2026. Bitcoin Improvement Proposal BIP-360 (proposing a quantum-resistant Pay-to-Merkle-Root output type) was merged into the BIP repository in February 2026, but has no confirmed activation pathway — and critically, BIP-360 does not replace ECDSA or Schnorr signatures with post-quantum alternatives. It only removes the Taproot key path exposure pattern. A full base-layer transition to PQ signatures requires a separate and much larger change. In April 2026, multiple competing post-quantum signature proposals are under active discussion — BIP-360 (P2MR key-path removal), SHRIMPS (2.5KB hash-based signatures, Jonas Nick / Blockstream Research), SHRINCS (324 bytes, stateful), Hourglass V2 (limits spending of exposed legacy coins to 1 BTC per block), and Tadge Dryja's commit/reveal scheme for mempool protection. Five proposals, no coordination, no consensus activation pathway for any of them. Ethereum's governance challenge has drawn significant commentary — but Bitcoin's coordination mechanism for changes of this scale has no equivalent of the Ethereum Foundation, no hard-fork framework, and as Nic Carter observed, "no one will admit that they have real influence over what gets implemented."

For institutional readers: the Bitcoin quantum risk is concentrated in custody and wallet infrastructure, not in the protocol consensus layer. Institutions holding BTC in custody should treat key rotation practices and the long-term viability of their signing infrastructure as first-order questions under a compressing CRQC timeline.

POST-QUANTUM RISK ON SOLANA — LIVE TESTNET CONFIRMS THE STRUCTURAL TRADEOFF

Solana hosts three of the most significant institutional programmes in this report: Visa's $3.5 billion annualized stablecoin settlement, WisdomTree's tokenized fund suite, and BUIDL's Solana share class. The Drift Protocol exploit at $285 million also occurred on Solana. A structural vulnerability that distinguishes Solana from Bitcoin and Ethereum: unlike chains where wallet addresses are typically derived from hashed public keys, Solana exposes public keys directly and by default across its entire address space.

> *"In Solana, 100% of the network is vulnerable. A quantum computer could pick any wallet and immediately start trying to recover the private key."*
>
> — Alex Pruden, CEO, Project Eleven (cryptography firm working with the Solana Foundation on post-quantum readiness), CoinDesk, April 4, 2026

This direct public-key exposure means Solana's at-rest attack surface is structurally wider than Ethereum's — where only wallets that have transacted expose their public key on-chain. For institutional programmes on Solana, every admin key, every governance signer, and every wallet associated with an institutional programme is an immediately accessible quantum attack surface, with no filtering by whether the wallet has ever transacted.

In April 2026, Project Eleven and the Solana Foundation published results from live testnet experiments replacing Solana's Ed25519 signatures with quantum-resistant alternatives. The results confirm the magnitude of the engineering challenge. Quantum-safe signatures are 20 to 40 times larger than current signatures. In live testing, a version of Solana using quantum-resistant cryptography ran approximately **90% slower** than its current throughput — a result that cuts directly at the foundation of Solana's commercial value proposition as the fastest institutional settlement rail in crypto.

> *"This is a tomorrow problem — until it's today's problem. And then it takes four years to fix."*
>
> — Alex Pruden, CEO, Project Eleven, April 4, 2026

Solana's ~400ms finality provides structural protection against on-spend attacks specifically — but offers zero protection against at-rest attacks on permanently and directly exposed admin keys, governance multisig signers, and Security Councils, as demonstrated by the $285 million Drift exploit. The live testnet data from Project Eleven confirms what modeled figures suggested: migrating Solana to quantum-safe cryptography imposes a commercially prohibitive throughput penalty on the current architecture. The Solana Foundation deserves credit for engaging on the problem — but engagement is not a roadmap, and a testnet that runs 90% slower is not a solution. For the three major institutional programmes currently operating on Solana, this gap requires an immediate strategic decision.

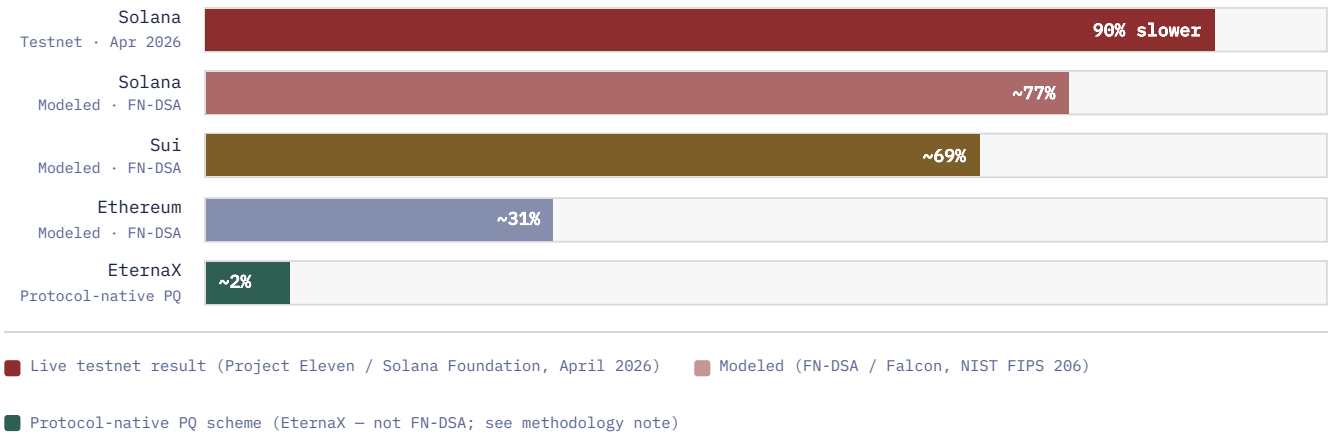
> *"Solana is going to have to rebuild everything from scratch. They've already massively optimized hardware around these signatures, which they're going to have to rip out and replace. If you're a very performant blockchain, it's actually a big problem — because now you have these slow, ugly, clunky signatures."*
>
> — Nic Carter, Co-Founder, Castle Island Ventures, Bankless Podcast, April 2026

> *"Active addresses that have already signed transactions must migrate before Q-Day because their public keys have been exposed."*
>
> — Circle Research, "How Blockchains Are Preparing for Q-Day," January 2026

TABLE 3.2 — TPS IMPACT UNDER POST-QUANTUM MIGRATION BY CHAIN: MODELED VS. LIVE TESTNET

CHAIN	MODELED TPS LOSS (FN-DSA)	LIVE TESTNET RESULT	PRIMARY INSTITUTIONAL PROGRAMMES	KNOWN PQ ROADMAP
Solana	**~77%**	**~90% (Project Eleven, Solana Foundation, Apr 2026)**	Visa stablecoin settlement, WisdomTree tokenized funds, BUIDL Solana share class, FOBXX Solana network	**None — testnet only, no mainnet roadmap**
Sui	**~69%**	No published testnet	Institutional DeFi, early RWA pilots	**None disclosed**
Ethereum	**~31%**	Devnets in progress	BUIDL (primary), MONY, FOBXX (ETH network), FYOXX, major stablecoin issuers	Partial — base-layer by 2029; contracts and L2s separate
EternaX	**~2%**	**Protocol-native; no retrofit required**	PQ-native issuance, migration destination rail	**Native — protocol-level information-theoretic scheme**

FIGURE 3.1 — TPS IMPACT UNDER POST-QUANTUM MIGRATION: SOLANA LIVE TESTNET VS. MODELED ESTIMATES



Methodology note: Modeled figures for Solana, Sui, and Ethereum use FN-DSA (Falcon, NIST FIPS 206) as the PQ signature replacement. The Solana live testnet figure (~90%) reflects Project Eleven and Solana Foundation testing published April 4, 2026 (CoinDesk). The signature size in live testing was 20–40× larger than current Ed25519 signatures. EternaX uses its own protocol-native 160-byte PQ scheme — not FN-DSA — and figures are not comparable across these methodologies. The qualitative directional claim — that chains designed PQ-native from inception materially outperform retrofitted chains on throughput — is robust under this caveat and is now confirmed by live data.

TABLE 3.3 — PQ SIGNATURE SIZE COMPARISON: INDUSTRY SCHEMES VS. ETERNAX PROTOCOL-NATIVE SCHEME

SCHEME	SIGNATURE SIZE	VS. ECC BASELINE	VS. ETERNAX	CURRENT STATUS
ECDSA / secp256k1 (Bitcoin, Ethereum)	65 bytes	Baseline	—	Quantum-vulnerable; current standard
Ed25519 (Solana, Stellar, Sui)	64 bytes	Baseline	—	Quantum-vulnerable; current standard
EternaX protocol-native PQ scheme	~160 bytes	2.5×	1× (baseline)	Information-theoretic; pending IACR publication
Falcon-512 / FN-DSA (Ethereum direction)	~690 bytes	~10.6×	4.3×	NIST FIPS 206; Ethereum exploring
Falcon-1024 (Algorand mainnet, Nov 2025)	~1,330 bytes	~20×	8.3×	Live on Algorand state proofs (opt-in); first major L1 PQ mainnet transaction
ML-DSA / CRYSTALS-Dilithium (NIST FIPS 204)	~2,420 bytes	~37×	15.1×	NIST standard; HSM-compatible
SLH-DSA-SHA2-128s (Circle Arc choice, Aptos AIP-137)	7,856 bytes	122×	49×	Chosen by Circle for Arc mainnet (April 2026, opt-in); Aptos AIP-137 proposal

What the signature size table means for throughput and institutional viability. Signature size is the primary driver of per-transaction bandwidth and block capacity. A chain using SLH-DSA-SHA2-128s signatures (Circle Arc's chosen scheme) must process 122× more bytes per signature than a chain using Ed25519 — or 49× more than EternaX's protocol-native scheme. At constant block sizes and validation throughput, this directly translates to proportional transaction-capacity reduction before any other computational overhead is considered. Circle's Arc blog confirms this is why validator hardening is deferred to a "long-term" phase: the performance implications of applying large-signature PQ schemes to the validator layer remain unresolved. EternaX's 160-byte scheme sits below the minimum 10× deterioration floor that Nic Carter cited as the industry's unavoidable cost of any NIST-compliant migration — and 49× smaller than the specific scheme the most credible institutional blockchain issuer just publicly chose.

Algorand: the first major L1 to complete a live PQ mainnet transaction. On November 3, 2025, Algorand broadcast the first mainnet transaction signed with Falcon-1024 — a NIST-selected lattice-based signature scheme. This was a significant milestone: proof that quantum-resistant signatures are deployable on a live public blockchain. Google's March 2026 paper explicitly cited Algorand's deployment as the closest existing real-world example of PQ adoption on a major L1. The important nuance for institutions: Algorand's Falcon-1024 deployment covers state proofs and is opt-in; core accounts still use Ed25519; full protocol-level migration remains on roadmap. The Falcon-1024 signature at ~1,330 bytes is 8.3× larger than EternaX's scheme. Algorand demonstrates the industry is moving — it does not demonstrate the full-stack institutional solution.

"Google made headlines with Bitcoin. The institutional story is Ethereum's $200 billion admin-control surface and Solana's 90% throughput loss confirmed in live testnet — both chains carrying the majority of the world's institutional tokenized-asset stack, with no PQ roadmap disclosed for any named programme."

SECTION 04

Why Tokenized Assets Should Not Inherit Avoidable Blockchain Rail Risk: *The Central Financial Argument*

This is the central financial argument of the report. Bitcoin's value is inseparable from the cryptographic network that secures it — rail risk is native and appropriate to price. That is not true of tokenized treasuries, stablecoins, tokenized money market funds, tokenized deposits, or most real-world assets. Their value comes from reserves, legal claims, fund structures, custodianship, sovereign credit, and regulated financial rights. The blockchain is the rail. When that rail is non-PQ-safe, a separate infrastructure choice contaminates otherwise clean financial claims with an avoidable future cryptographic liability.

TABLE 4.1 — NATIVE CRYPTO ASSETS VERSUS TOKENIZED OFF-CHAIN ASSETS: WHY RAIL CONTAMINATION REGISTERS DIFFERENTLY

CATEGORY	VALUE SOURCE	HOW RAIL CONTAMINATION REGISTERS
Native cryptoassets (BTC, ETH)	Network belief, token economics, cryptographic scarcity	Rail risk is native — asset and rail are the same system; risk premium is legitimate
Fiat-backed stablecoins	Off-chain cash reserves, redemption rights, issuer governance	Rail contamination is an imported liability — a dollar-backed asset should not carry a blockchain-native cryptographic risk premium
Tokenized MMFs (BUIDL, FOBXX, MONY, FYOXX)	U.S. Treasury securities, administrator, custodian, legal claim	Wrong rail adds migration complexity, control-plane fragility, and privacy contamination to an asset backed by U.S. government securities
Tokenized deposits / bank liabilities	Bank liability structure, deposit framework, legal entitlement	Rail contamination is external to the underlying banking claim
Most real-world assets	Physical asset, enforceable rights, underlying economic reality	The blockchain should add efficiency. It should not add a permanent cryptographic liability the asset class never carried in traditional markets.

> *"We are excited to be a first mover with the launch of MONY, and we expect other G-SIB banks to follow our lead in providing clients with greater optionality in how they invest in money market funds on blockchain."*
>
> — John Donohue, Head of Global Liquidity, J.P. Morgan Asset Management, December 15, 2025

Donohue is right that other G-SIBs will follow. The question for each institution following JPMorgan's lead is not whether to issue a tokenized money market fund. The question is which rail to issue it on — and whether that rail imports a cryptographic contamination into an asset backed by U.S. Treasury securities and banking-grade custody.

"A stablecoin backed 1:1 by dollars should not trade at a rail-induced discount. A tokenized Treasury fund backed by U.S. government securities should not absorb migration debt and privacy contamination because of a blockchain infrastructure decision made at issuance."

SECTION 05

Institutional Blockchain Quantum Risk: *The Enterprise-to-Rail Trace for Named Programmes*

Naming institutions is not enough. The exposure becomes concrete only when you trace the complete chain: enterprise → product → counterparties → control surfaces → privacy surfaces → rail.

TRACE 01 — BLACKROCK BUIDL ($2.85B AUM)

Enterprise → Product → Counterparties → Control Surfaces → Privacy Surfaces → Rail

ENTERPRISE	PRODUCT	COUNTERPARTIES	CONTROL SURFACES	PRIVACY SURFACES	RAIL
BlackRock ($14T AUM)	BUIDL Fund ($2.85B)	Securitize (transfer agent, tokenization) · BNY Mellon (custodian) · Wormhole (cross-chain interop)	Securitize transfer-agent signing keys · BNY custody keys · BUIDL contract upgrade authority · Wormhole bridge attesters · Admin keys across 9 blockchains	Public-chain visibility across 9 public chains · DeFi integrations publicly observable · All investor wallet activity visible on-chain	secp256k1 / Ed25519 on all 9 chains · No disclosed PQ roadmap at any node in this stack

The key insight: BUIDL's $2.85 billion in AUM represents a claim on U.S. Treasury bills, repurchase agreements, and cash. That underlying value is unaffected by quantum computing. What is affected is the entire chain of authorization, transfer-agent governance, cross-chain interoperability, and investor privacy above it. Securitize's transfer-agent signing perimeter controls the official record of share ownership — if compromised, the official ownership record is attackable regardless of how clean the underlying Treasury securities are.

TRACE 02 — VISA STABLECOIN SETTLEMENT ($3.5B+ ANNUALIZED)

Enterprise → Product → Counterparties → Control Surfaces → Privacy Surfaces → Rail

ENTERPRISE	PRODUCT	COUNTERPARTIES	CONTROL SURFACES	PRIVACY SURFACES	RAIL
Visa (200+ countries)	USDC Stablecoin Settlement (U.S. banks + acquirers)	Stablecoin issuer · Cross River Bank · Lead Bank · (broader U.S. rollout through 2026)	Stablecoin mint/burn admin keys (governs ~$200B admin-vulnerable assets per Google) · Visa settlement authorization · USDC CCTP signing perimeter · Bank settlement wallet keys	All settlement flows permanently visible on public Solana · Bank-to-bank volumes, timing, and counterparty relationships publicly observable	Solana Ed25519 · No disclosed PQ roadmap for Visa settlement infrastructure, the stablecoin issuer, or Solana

The stablecoin issuer's admin keys do not merely govern the circulating supply. They govern the minting authority for a token used in Visa's settlement infrastructure, BUIDL's subscription and redemption mechanics, JPMorgan MONY's investor off-ramps, and hundreds of institutional DeFi integrations simultaneously. A successful attack on those admin keys is not a stablecoin problem — it is a settlement infrastructure problem at the scale of major global payment networks.

TRACE 03 — DTCC TOKENIZATION SERVICE (COVERS $100T+ DTC CUSTODY BASE)

Enterprise → Product → Counterparties → Control Surfaces → Privacy Surfaces → Rail

ENTERPRISE	PRODUCT	COUNTERPARTIES	CONTROL SURFACES	PRIVACY SURFACES	RAIL
DTCC / DTC ($100T+ custody)	DTC Tokenization Service (H2 2026): Russell 1000, U.S. Treasuries, major-index ETFs	Digital Asset (Canton Network) · DTC Participants · Euroclear (Canton co-chair)	DTC override keys (can reverse transactions or destroy tokens) · DTC Factory minting system · Canton Network governance · Participant wallet registration	Canton provides configurable privacy but underlying cryptographic assumptions remain subject to quantum threat; Canton PQ posture undisclosed	Canton Network — PQ criteria for approved blockchains not publicly disclosed as of April 2026

DTC's override key infrastructure — the master keys that can reverse transactions and destroy tokens — becomes a critical control surface for U.S. capital markets when tokenized entitlements of Russell 1000 equities, U.S. Treasuries, and major ETFs begin trading on public blockchains from H2 2026. The fact that PQ criteria for approved Canton blockchains have not been publicly disclosed is a gap the industry should ask to be addressed before H2 2026 rollout begins.

TRACE 04 — THE CUSTODIAN / DEFI PROTOCOL / ORACLE OPERATOR (SELF-APPLICATION TEMPLATE)

For every entity in Table 6.1 not covered by Traces 01–03: how to apply this framework to your own stack

YOUR ENTERPRISE	YOUR PRODUCTS	YOUR COUNTERPARTIES	YOUR CONTROL SURFACES	YOUR PRIVACY SURFACES	YOUR RAIL
Custodian · DeFi Protocol · Oracle Provider · Market Maker · Prime Broker · Tokenization Platform · Lending Protocol · Exchange	Custody vaults · Protocol TVL · Price feed infrastructure · Market-making positions · Client collateral · Issued tokens · Loan books · Spot / derivatives positions	Who are your upstream signers? Whose keys govern assets you custody, attest, price, or intermediate? Whose PQ roadmap are you dependent on?	Custody master keys · Oracle signer keys · Protocol admin multisig · Bridge attester keys · Governance vote keys · Upgrade proxy authority · Liquidation bot signing perimeter	On-chain position visibility · Flow timing · Counterparty relationships · Strategy and rebalancing patterns · Oracle update cadence and signer identity	Which chains do your products settle on? Do those chains have disclosed PQ roadmaps? Do your signing perimeters expose public keys permanently on-chain?

The three questions every entity in Table 6.1 must answer about their own stack: First — which of my signing keys are permanently exposed on-chain, and what is the total value they govern directly and through upstream dependencies? Second — does my primary settlement rail have a credible PQ roadmap that covers not just the base-layer protocol but also my layer of the stack (smart contracts, oracle feeds, bridge attestation, custody key management)? Third — for the assets or workflows I am creating or expanding today, am I knowingly creating fresh migration debt that will require expensive coordinated migration later? These three questions applied to any entity in Table 6.1 will produce the same answer this report produces for BlackRock, Visa, and DTCC: material exposure at the control plane, no credible PQ roadmap covering the full stack, and a compounding window to act before architecture lock-in.

SECTION 06

Nine Named Institutional Programmes, *Zero Disclosed Post-Quantum Roadmaps*

TABLE 6.1 — FULL INSTITUTIONAL AND INFRASTRUCTURE UNIVERSE IN SCOPE

CATEGORY	REPRESENTATIVE ENTITIES	EXPOSURE PRIORITY
Traditional allocators and on-ramp builders	Apollo, Millennium, KKR, Fidelity, Goldman Sachs, UBS, Standard Chartered, BlackRock, Franklin Templeton, WisdomTree, BNY Mellon, J.P. Morgan, Citi, State Street, BNP Paribas, Visa, Stripe/Bridge, Paxos, Ripple, DTCC, Nasdaq, NYSE/ICE, CME Group, SIX/SDX, Swift, Euroclear, Clearstream, Taurus	ASSET CONTROL
Custody and key management	Fireblocks, Anchorage Digital, BitGo, Copper, Zodia, Coinbase Custody, Fidelity Digital Assets Custody	CONTROL Master key exposure — critical path
Prime brokerage and execution	FalconX, Coinbase Institutional/Prime, Hidden Road, LMAX Digital, Galaxy Digital	CONTROL PRIVACY
Market makers and liquidity	Keyrock, Wintermute, B2C2, GSR, Optiver, CMT Digital, Jump Trading	ASSET PRIVACY Strategy / flow visibility

CATEGORY	REPRESENTATIVE ENTITIES	EXPOSURE PRIORITY
Tokenization, issuance, and data layers	Securitize, Paxos, Chainlink, Tokeny, Zoniqx, Canton Network/Digital Asset, Ondo Finance	CONTROL BRIDGE Transfer agent + oracle keys — critical path
Risk, curation, and staking	Gauntlet, Steakhouse, Sentora, Bitwise, Figment, P2P.org, Lido (~20% staked ETH), Nansen, The Tie	CONTROL Lido: 20% staked ETH concentration
Crypto-native banks	Amina Bank, Sygnum, Xapo, Bank Frick, Matrixport, Bergos AG	CONTROL PRIVACY
Yield, credit, and on-chain finance layers	Ondo, Ethena, Centrifuge, Backed, Sky, Maple, Goldfinch, Clearpool, Open Eden, Morpho, Aave, Compound, Spark, Kamino, Curve, Notional, Pendle	ASSET CONTROL Accept collateral governed by admin-vulnerable keys
Settlement, execution, and network rails	Ethereum, Solana, Hyperliquid, Canton, Stellar, XRPL, Polygon, Avalanche, Aptos, Arbitrum, Optimism, Base	ASSET CONTROL PRIVACY Full-stack exposure — all three planes

TABLE 6.2 — NAMED INSTITUTIONAL PROGRAMMES: RAILS, DEPENDENCIES, AND POST-QUANTUM POSTURE

PROGRAMME	SCALE	PRIMARY RAIL(S)	KEY DEPENDENCIES	PRIMARY PQ EXPOSURE	PQ ROADMAP?
BlackRock BUIDL	~$2.85B AUM; 9 chains; $100M+ dividends paid; largest tokenized RWA fund globally	Ethereum (primary), Solana, Arbitrum, Aptos, Avalanche, BNB Chain, Optimism, Polygon	Securitize (transfer agent), BNY (custodian), Wormhole (interop)	ASSET CONTROL BRIDGE 9 chains; Securitize signing; bridge attesters	**None disclosed**
Franklin FOBXX (Benji)	First U.S.-registered mutual fund on public blockchain (2021); $594M+ AUM; 9+ networks	Stellar (primary), Polygon, Arbitrum, Avalanche, Aptos, Ethereum, Solana, Base, Canton	Franklin Templeton Investor Services (transfer agent, Benji platform)	CONTROL PRIVACY Transfer agent governs approved wallets across 9 rails	**None disclosed**
JPMorgan MONY	Launched December 15, 2025; $100M JPMorgan seed; first G-SIB tokenized MMF on public chain	Ethereum (Kinexys Digital Assets); JPM Coin on Base; Canton planned 2026	Kinexys Digital Assets, Morgan Money distribution, stablecoin settlement	ASSET CONTROL Kinexys admin signing; expanding to Canton 2026	**None disclosed**
WisdomTree Tokenized Funds	Full suite on Solana from January 2026; institutional + retail; self-custody portability	Solana (primary); WisdomTree Connect + Prime	WisdomTree Connect, Prime, stablecoin settlement rails	ASSET PRIVACY Solana direct key exposure; investor self-custody	**None disclosed**
Visa Stablecoin Settlement	$3.5B+ annualized (Nov 30, 2025); U.S. launch December 2025; Cross River Bank and Lead Bank live	Solana (U.S.); global pilots across LAC, Europe, APAC, CEMEA	Stablecoin issuer, Cross River Bank, Lead Bank	ASSET CONTROL PRIVACY Settlement flows on public Solana; stablecoin admin keys	**None disclosed**

PROGRAMME	SCALE	PRIMARY RAIL(S)	KEY DEPENDENCIES	PRIMARY PQ EXPOSURE	PQ ROADMAP?
DTCC Tokenization Service	SEC no-action letter Dec 11, 2025; H2 2026 launch; $100T+ DTC custody base; Russell 1000, Treasuries, ETFs	Canton Network (Digital Asset partnership); DTCC co-chairs Canton Foundation with Euroclear	Digital Asset (Canton), ComposerX, DTC participant wallet registration	CONTROL DTC override keys; Factory minting; Canton PQ undisclosed	**No PQ criteria disclosed**
Major stablecoin issuers	~$265B combined circulation; 30+ networks; $33T 2025 transaction volume; 7th-largest purchasers of U.S. Treasuries	Ethereum, Solana, and 28+ others	Issuer stack, custodian reserves, cross-chain transfer infrastructure	ASSET CONTROL BRIDGE Minting authority keys; CCTP signing perimeter; 30+ rails	**None disclosed**
Fidelity FYOXX	Launched mid-2025; first on-chain tokenized product from $5.9T AUM manager; Ethereum	Ethereum (current); additional chains per SEC filing in development	Fidelity Digital Asset Management; Ethereum transfer agent infrastructure	ASSET CONTROL Ethereum key exposure; transfer agent signing	**None disclosed**
Fidelity Digital Dollar (FIDD)	Launched February 4, 2026; new institutional stablecoin issued by Fidelity Digital Assets, NA; 1:1 USD-backed, backed by cash/U.S. Treasurys; available retail and institutional; purchasable/redeemable at $1; transferable to any Ethereum mainnet address	Ethereum mainnet; transferable to any ETH address	Fidelity Digital Assets, NA (issuer); Fidelity reserve management; Fidelity platform distribution; daily supply and reserve NAV disclosure	ASSET CONTROL PRIVACY **Live Feb 2026 — new issuance on non-PQ-safe rail**	**None disclosed**

MARKET POSTURE ASSESSMENT · APRIL 2026

Nine named institutional programmes. Combined assets under management, administration, or settlement custody exceeding $3.2 trillion directly connected to these rails. Total stablecoin market of $317 billion, $36 billion in tokenized RWAs (ex-stablecoins), and $33 trillion in 2025 stablecoin transaction volume — all on quantum-vulnerable infrastructure. Zero end-to-end post-quantum roadmaps disclosed covering custody, admin controls, settlement mechanics, interoperability, and audit across any of the nine named programmes. That is the current posture of institutional on-chain finance with respect to post-quantum preparedness.

> *"This is something we're going to have to look into. I'm personally looking into this."*
>
> — Brian Armstrong, CEO, Coinbase, April 6, 2026 — publicly acknowledging the quantum threat the same day this report was published

Brian Armstrong's April 6, 2026 statement is notable not because it resolves anything — Coinbase has disclosed no PQ roadmap for its custody infrastructure, its exchange, or its L2 (Base). It is notable because the CEO of the largest publicly traded crypto company is now personally engaged. That engagement is the first acknowledgement from major exchange

leadership that the quantum problem requires CEO-level attention. It is not a roadmap. It is the acknowledgement that a roadmap is needed. The verdict box above remains accurate: zero end-to-end PQ roadmaps disclosed across all named programmes.

> *"Nine named institutional programmes. Zero disclosed end-to-end post-quantum roadmaps. The infrastructure is live, operational, and growing every week. The migration plans are not."*

> ***"This affects real institutions conducting real operations on real rails — not crypto traders."***

SECTION 07

Control-Plane Vulnerability in Crypto: *Where Institutional Risk Actually Concentrates*

Post-quantum risk is not a wallet problem. For enterprises, the control plane is the primary exposure — admin keys, governance multisigs, upgrade authorities, transfer-agent signing perimeters. These surfaces govern far more value than the ETH they directly hold, because they control the logic sitting above billions in tokenized assets. A quantum computer does not need to steal a wallet to drain an institutional programme. It needs to crack the key that controls the contract that governs the fund.

TABLE 7.1 — WHERE INSTITUTIONAL CONTROL-PLANE RISK CONCENTRATES

SURFACE	WHAT IT CONTROLS	PQ RISK
Mint/burn authority	Can create or destroy token supply; governs on-chain representation of reserve-backed assets	Unlimited token creation decoupled from reserves; balance sheet attack at stablecoin issuers
Freeze/blacklist authority	Can restrict or immobilize balances; governs compliance enforcement	Illegitimate freezes impair counterparty relations; selective freeze creates market panic
Upgrade authority	Can alter contract logic, pause systems, or override constraints across all token holders simultaneously	Logic replacement enabling fund redirection; silent drain of collateral pools
Transfer-agent governance	Controls official ownership record and approved-wallet state; governs who is recognized as a legal holder	Fraudulent ownership record; unauthorized wallet approval; regulatory compliance compromise
Bridge/attestation signers	Determine cross-chain transfer semantics and wrapped-asset backing across the bridge's entire locked value	Forged bridge messages; drained wrapped-asset reserves; cross-chain double-spend at bridge scale

SURFACE	WHAT IT CONTROLS	PQ RISK
Security Council multisigs	Emergency pause, contract upgrade, parameter changes for DeFi protocols governing billions in TVL	Protocol takeover enabling asset drain — see Drift case study
DTC override keys	DTC retains unilateral authority to reverse transactions and destroy tokenized entitlements for U.S. capital markets tokenized settlement	Override authority for the entire U.S. capital markets tokenized settlement layer; highest-stakes control surface in this report

CONTROL-PLANE CASE STUDY — PRESENT COST VS. POST-QUANTUM COST

The Drift Protocol Exploit: $285 Million, Social Engineering, and What Changes Under Quantum Threat

$285–286M	April 1, 2026	~12 minutes	~3 weeks	DPRK-attributed
Assets drained	Execution date	Execution window	Staging (from March 11)	Elliptic, TRM Labs

On April 1, 2026, Drift Protocol — the largest decentralized perpetuals exchange on Solana, with ~$550 million in TVL — was drained of approximately $285 to 286 million in approximately twelve minutes. Largest DeFi hack of 2026. Second-largest in Solana history. Attributed to DPRK-linked actors by Elliptic and TRM Labs, with attribution ongoing as of publication.

The attack did not exploit a smart contract vulnerability. It exploited governance and signing processes. The attacker abused "durable nonces" — a legitimate Solana feature overriding the normal 60–90 second transaction expiry — to pre-sign transactions that remained valid indefinitely. By social engineering two of five Security Council multisig members into approving those transactions, the attacker triggered a complete governance takeover in twelve minutes, draining all user deposits. The Security Council had been changed to 2-of-5 without a timelock weeks earlier, removing the last automated defense. A fake token (CarbonVote/CVT), seeded with minimal liquidity, was presented to oracles as legitimate collateral worth hundreds of millions.

The post-quantum relevance is precise. Reaching Drift's control plane required three weeks of preparation, the manufacture of a fake token ecosystem, and the social engineering of two security council members. Under a quantum-capable threat model, the social engineering requirement is eliminated for control surfaces whose signers' public keys are permanently exposed on-chain. A CRQC converts a three-week social engineering operation into a direct cryptographic computation. The attack becomes faster, cheaper, and independent of human psychology. Institutions should read this not as "quantum eliminates social engineering" but as: quantum eliminates the requirement for social engineering on cryptographically vulnerable key surfaces.

Sources: Elliptic, TRM Labs, CoinDesk, Bloomberg (April 1–3, 2026). DPRK attribution ongoing as of publication.

"Reaching Drift's control plane cost three weeks and required social engineering two humans. Under quantum threat, the social engineering step is eliminated for exposed key surfaces. The $200 billion in stablecoin and RWA admin-control exposure on Ethereum is the institutional-scale version of that same surface."

SECTION 08

Blockchain Privacy Durability and the Post-Quantum Privacy Risk:

Retroactive Degradation, Harvest-Now-Decrypt-Later, and Auditable Privacy for Institutional Digital Assets

Privacy-preserving blockchains will degrade retroactively under quantum attack. Google's March 2026 paper makes this explicit. The word "retroactive" is what matters: historical transaction data that appears private today becomes readable in the future as quantum capabilities improve. The privacy was real when the transaction occurred. It will not be real when a quantum computer arrives with the stored record.

State actors are already collecting blockchain data with no intention of decrypting it now. An adversary who collects data in 2026 and decrypts it in 2031 has effectively travelled back in time to observe 2026 transactions as if conducted in the clear. For on-chain institutional finance, where the ledger is permanent and every transaction irreversibly recorded, this threat has no expiry date and no remediation once the data is on-chain.

CONCRETE INSTITUTIONAL SCENARIO — HARVEST NOW, DECRYPT LATER

Consider a treasury desk at a major stablecoin issuer executing on-chain collateral movements in Q3 2026. The transactions record on Ethereum's public ledger: counterparty addresses, amounts moved, routing between protocols, timing. Today, that data is protected by secp256k1 assumptions.

In 2031 or 2033, those assumptions may not hold. An adversary who collected and stored that 2026 data now holds the complete strategic record of that treasury desk's Q3 2026 operations: positions, counterparties, rebalancing timing, collateral strategy, the identity of every wallet involved. The transaction already occurred. The data is permanently on-chain. The cryptographic protection that appeared adequate in 2026 is what is being retroactively broken — not the transaction itself.

TABLE 8.1 — PRIVACY MODELS AND THEIR INSTITUTIONAL DURABILITY

PRIVACY MODEL	WHAT IT PROVIDES TODAY	WHAT IT FAILS TO PROVIDE	ASSESSMENT
Public-by-default (Ethereum, Solana)	Transparency and composability for all market participants	Balance, flow, and strategy confidentiality for all market participants simultaneously	Inadequate for institutional treasury, fund management, or sensitive counterparty workflows
Permissioned/configurable (Canton)	Controlled visibility within defined participant groups; better operational privacy	Not automatically PQ-safe; underlying cryptographic assumptions remain; Canton PQ posture undisclosed	Better than public, but requires verification of underlying scheme durability
Privacy overlay/shielded (Zcash, Monero model)	Better present-state confidentiality; obfuscated transaction graph	Zcash Sapling trusted setup vulnerable to on-setup quantum attack; Monero ring signatures use Ed25519 (quantum-vulnerable); retroactive exposure risk for all historical shielded transactions; no compliance-ready selective disclosure	Inadequate for institutions requiring audit, compliance, and regulatory disclosure alongside confidentiality. Not PQ-safe.

PRIVACY MODEL	WHAT IT PROVIDES TODAY	WHAT IT FAILS TO PROVIDE	ASSESSMENT
Obfuscation-based	Reduced immediate readability	Machine learning already degrades obfuscation; quantum compounds this; not durable	Not a long-term institutional solution
Auditable-private with PQ-safe foundations	Hidden flows with selective disclosure for compliance; verifiable settlement without broadcasting counterparty or strategy data	Requires information-theoretic or PQ-safe cryptographic foundations to be truly durable; security model must be proved, not assumed	The correct institutional direction — confidentiality, compliance, and cryptographic durability simultaneously. The only model that satisfies all three.

TABLE 8.2 — WHY INSTITUTIONS NEED PQ-SAFE AUDITABLE PRIVACY: THE FOUR-REQUIREMENT CASE

INSTITUTIONAL NEED	WHY PUBLIC RAILS FAIL	WHY PRIVACY CHAINS FAIL	WHY PQ-SAFE AUDITABLE-PRIVATE DESIGN MATTERS
Hidden treasury operations	Balance, flow timing, and counterparty relationships permanently visible on-chain — any analyst can reconstruct treasury strategy in real time	Zcash on-setup quantum attack retroactively compromises all shielded transactions; Monero uses Ed25519 (quantum-vulnerable); Arc defers privacy to post-mainnet	Hidden flows with information-theoretic durability — today's treasury movements cannot be retroactively decoded regardless of future computational advances
Trading intent confidentiality	Strategy is permanently visible on-chain before, during, and after execution — front-running, imitation, and counterparty inference all trivially enabled	Hard-privacy chains create compliance friction and lack selective disclosure — cannot satisfy both confidentiality and supervisor transparency simultaneously	Hidden trading positions and flows, with selective disclosure to compliance functions on demand — not traded off against each other
Counterparty confidentiality	Wallet clustering and on-chain flow inference permanently exposes counterparty relationships — observable by any market participant with analytics access	Retroactive exposure risk for all historical data; Zcash and Monero cannot guarantee that 2026 counterparty data stays hidden in 2031 under quantum attack	Counterparty relationships hidden from market participants, quantum-durably — harvested data yields nothing to a future quantum-capable adversary
Regulatory transparency on demand	Public rails provide too much transparency to everyone — not selective disclosure to supervisors while maintaining market confidentiality	Hard-privacy rails fail supervisors — compliance-grade selective disclosure requires architectural support that privacy-overlay chains do not provide	Selective disclosure to regulators, auditors, and compliance functions — simultaneously with confidentiality from market participants — built in at the architecture layer

INSTITUTIONAL NEED	WHY PUBLIC RAILS FAIL	WHY PRIVACY CHAINS FAIL	WHY PQ-SAFE AUDITABLE-PRIVATE DESIGN MATTERS
Investor identity protection	Wallet-to-entity linkage trivially available through on-chain analytics — investor identities and positions permanently observable	Computationally-secure privacy chains offer protection today; under quantum attack, historical investor identity data is retroactively exposed from the permanent on-chain record	Information-theoretically private investor identity data — not protected by computational assumptions that a quantum computer could eventually break

"PQ-safe auditable privacy is not a feature. It is the only architecture where long-duration institutional capital can be held on-chain with confidentiality that does not expire and compliance that is built in — not traded against each other."

The critical distinction institutions miss: signing-layer PQ and privacy-layer PQ are not the same thing. Most discussions of post-quantum migration focus exclusively on replacing ECDSA and Ed25519 signatures with quantum-resistant alternatives. This addresses the authorization layer — who can move assets. It does not address the privacy layer — what adversaries can observe and decode from the permanent on-chain record.

A chain that migrates its signing keys to NIST post-quantum standards but continues to record transaction flows, balances, and counterparty relationships under computationally-secure privacy assumptions has solved half the problem. An adversary running Shor's algorithm on historically collected transaction data does not need to forge a signature. They need only to break the cryptographic assumptions protecting the privacy of what was already recorded. On Ethereum and Solana, transactions are public-by-default — no privacy to break. On Zcash, the Sapling trusted setup is itself vulnerable to an on-setup quantum attack, retroactively compromising all shielded transactions. On Monero, ring signatures use Ed25519 — quantum-vulnerable. Circle's Arc has deferred privacy to a "near-term" post-mainnet roadmap item.

The only architecture with quantum-durable privacy at both layers requires information-theoretic or post-quantum cryptographic foundations applied to the privacy model itself — not just applied to signing keys. That architecture is the final row of Table 8.1. It is the architecture that matters for long-duration institutional finance, where harvested data from 2026 may be decrypted in 2031, 2035, or 2040.

SECTION 09

Migration Debt in Blockchain and Tokenized Finance: *What It Contains and When It Starts Accruing*

Migration debt is not a metaphor. It is a concrete and compounding set of costs that accumulates when long-duration value is issued on rails whose authorization model, control surface, and privacy architecture are not future-safe. It begins accruing the moment an asset is issued, not the moment an attack occurs. It compounds on success, not on failure — every new counterparty, DeFi integration, and client relationship deepens it. Every expansion makes it worse. The window for cheap correction closes as the programme scales.

TABLE 9.1 — THE COMPONENTS OF CRYPTOGRAPHIC MIGRATION DEBT

COMPONENT	MEANING	HOW IT COMPOUNDS
Coordination debt	Custodians, transfer agents, exchanges, clients, and venues must move together in a coordinated re-platforming event	Every new counterparty adds a stakeholder whose consent and technical capability must be obtained simultaneously
Contract debt	Issuer contracts, admin rights, redemption mechanics, proxy upgrade logic, and legal structures must be redesigned	Legal re-issuance, smart contract replacement costs, and client contractual lock-in all compound with AUM scale
Liquidity debt	Assets bifurcate into old and new forms during migration, impairing pricing uniformity and DeFi composability	The longer the migration takes, the wider the bifurcation
Vendor debt	Supplier timelines and capabilities govern the migration floor; slowest critical-path vendor determines when migration can complete	Every new vendor relationship on vulnerable rails adds a dependency requiring simultaneous migration
Privacy debt	Historic transaction data on public rails cannot be retroactively shielded; harvest-now-decrypt-later attack surface grows with every transaction	Accumulates permanently and irreversibly; there is no "un-transacting" the on-chain record
Audit and governance debt	Board approvals, risk-committee disclosures, regulatory filings, and investor communications must all be revisited during migration	Every governance artifact based on current architecture must be renegotiated during migration
Reputation debt	Boards and clients will ask why weak rails kept being used after warnings, standards, and government guidance were publicly available	The public warning record is now substantial: NIST FIPS August 2024, Google March 2026, NCSC milestones. "We didn't know" is no longer available as a defense.

> *"This is a tomorrow problem — until it's today's problem. And then it takes four years to fix."*
>
> — Alex Pruden, CEO, Project Eleven, CoinDesk, April 4, 2026 — on the cost of deferred migration planning for blockchain infrastructure

---

"Migration debt compounds on success, not on failure. Every tokenized fund that grows, adds chains, attracts DeFi integrations, and expands to new counterparties is deepening its migration complexity simultaneously. The window for low-cost migration closes as the programme scales."

SECTION 10

Post-Quantum Decision Framework for Institutions: *Legacy Exposure Versus New Issuance*

TABLE 10.1 — LEGACY EXPOSURE VERSUS NEW ISSUANCE: WHAT EACH REQUIRES

CATEGORY	MEANING	CORRECT INSTITUTIONAL RESPONSE	URGENCY
Legacy exposure already live	Existing products and workflows on quantum-vulnerable rails	Contain and ring-fence; harden control-plane perimeter immediately; build migration plan; engage all critical suppliers on PQ roadmaps	High: start now
Existing programme being expanded	A live programme extended to more chains, clients, venues, or geographies	Each expansion is a fresh migration-debt creation event. Treat as new issuance, not as legacy continuation.	Very high: each expansion is a compounding choice
New issuance	New stablecoins, tokenized funds, tokenized deposits, tokenized securities, or treasury rails designed today	Do not issue on rails that create avoidable migration debt. The cost of PQ-native issuance today is a fraction of migrating an established programme later.	Immediate: entirely a choice, not an inheritance
Pilot likely to become production	Current experiments on potentially vulnerable rails that will likely scale to institutional significance	Use pilots to test destination architecture. A successful pilot on a vulnerable rail becomes the production architecture by default unless an alternative is specified from inception.	High: the production assumption solidifies before the pilot ends

Legacy exposure may require years of managed migration. New issuance is entirely a choice. No board wants to be told in 2030 that in April 2026 — with NIST standards finalized, government milestones published, Google's paper in the public record, and the Ethereum Foundation acknowledging the urgency — their programme knowingly created fresh migration debt for long-duration assets on documented vulnerable rails.

TABLE 10.2 — BOARD DECISION MATRIX: WHAT EACH INSTITUTION TYPE SHOULD DO IN THE NEXT 90 DAYS

IF YOU HAVE…	RISK LEVEL	IMMEDIATE ACTION (NOW)	WHAT TO AVOID	90-DAY DECISION
Legacy stablecoin or tokenized fund already live on Ethereum or Solana	**Critical**	Inventory all admin keys, mint/burn/freeze authority, and transfer-agent signing perimeters. Map which are permanently exposed on-chain. Begin control-plane hardening immediately.	Any further expansion — new chains, new DeFi integrations, new client relationships — deepens migration debt	Define migration route. Evaluate PQ-native issuance rails for any next-generation programme. Set board-level PQ risk mandate.
New stablecoin or tokenized product currently in architecture design (e.g., FIDD, PYUSD expansion, new tokenized fund)	**Immediate**	Pause architecture lock-in. Evaluate PQ-native rails before committing to legacy infrastructure. The cost of evaluation is a fraction of the cost of migrating an established programme.	Issuing on legacy rails after April 2026 is a knowing choice to create avoidable migration debt	Define rail selection criteria including full PQ rubric. Evaluate EternaX and other PQ-native architectures before committing.

IF YOU HAVE…	RISK LEVEL	IMMEDIATE ACTION (NOW)	WHAT TO AVOID	90-DAY DECISION
Tokenized fund across multiple chains (BUIDL, MONY, FOBXX model)	**High**	Map all transfer-agent, bridge, and oracle dependencies across every active chain. Block any new chain expansion until migration plan exists.	Each new chain is a compounding migration-debt event — treat every expansion as a board-level decision, not a technical default	Define per-chain migration priority. Separate high-value institutional share classes for earliest migration. Require vendor PQ roadmaps from all critical-path suppliers.
Public-chain treasury or stablecoin settlement flows (Visa, JPMorgan JPMD model)	**High**	Privacy review of all on-chain settlement flows. Map treasury movement visibility. Assess whether on-chain settlement creates competitive intelligence exposure under HNDL threat model.	Expanding public-chain settlement volumes without understanding the privacy exposure that data creates under quantum threat	Evaluate auditable-private settlement rails. Define minimum privacy requirements for any new on-chain settlement architecture.
Custody or key management for institutional digital assets	**High**	Inventory all key types and their on-chain exposure. Require PQ roadmap from every key-management vendor. Classify master keys, omnibus keys, and client-specific keys by exposure level.	Renewing long-term key-management vendor contracts without PQ disclosure requirements	Define institution-wide PQ key management standard. Begin RFP process for PQ-capable custody infrastructure.

TABLE 10.3 — PER-ENTITY ACTION PLAN: THIS WEEK · IN 90 DAYS · STOP NOW

IF YOU ARE…	DO THIS WEEK	DO IN 90 DAYS	STOP IMMEDIATELY
Stablecoin issuer USDC, FIDD, PYUSD, Tether	Map every admin key — mint, burn, freeze, upgrade — and its on-chain exposure status. Assign ownership. Set board-level mandate for PQ risk.	Require PQ roadmap from every custodian, transfer agent, and bridge you depend on. Define rail criteria for any future product launch. Begin migration-debt inventory across all active programmes.	**Stop expanding existing programmes to new chains or DeFi integrations without a board decision on compounding migration debt. Stop issuing new stablecoins on legacy rails without evaluating PQ-native alternatives.**
Tokenized fund manager BUIDL, MONY, FOBXX, FYOXX	Map all transfer-agent, bridge, oracle, and custodian dependencies across every active chain. Identify which are on-chain key-exposed control surfaces.	Require end-to-end PQ roadmap from Securitize or equivalent transfer-agent provider. Block any new chain expansion pending migration plan. Evaluate PQ-native issuance rails for next fund launch.	**Stop adding chains, institutional share classes, or DeFi protocol integrations to existing programmes without treating each as a compounding migration-debt event requiring board approval.**

IF YOU ARE…	DO THIS WEEK	DO IN 90 DAYS	STOP IMMEDIATELY
Custodian BitGo, Anchorage, Coinbase Custody, Fidelity DA	Inventory all key types — HSM, cold, warm, omnibus, client-specific — and their on-chain exposure status. Identify every vendor in your signing supply chain.	Require NIST FIPS 203/204/205 evaluation from every key-management vendor. Define institution-wide PQ key management standard. Begin RFP for PQ-capable custody infrastructure.	**Stop renewing long-term key-management and custody vendor agreements without binding PQ roadmap disclosure requirements. A vendor with no answer is your migration floor.**
Exchange / trading venue Coinbase, Binance, Hyperliquid, OKX	Inventory all hot-wallet, settlement-wallet, and treasury-key exposure. Identify which signing keys are permanently on-chain. Assign PQ risk ownership.	Require PQ attestation from every institutional custodian counterparty. Model throughput impact of PQ migration on settlement workflows. Define minimum PQ criteria for new chain integrations.	**Stop treating the quantum risk as only a user-wallet problem. Hot-wallet and omnibus key exposure is the institutional-scale control-plane risk.**
Tokenization platform Securitize, Fireblocks, Tokeny	Define your PQ migration posture for admin-control logic, transfer-agent signing, and upgrade-authority keys. Identify every client asset governed by your exposed keys.	Publish a workflow-level PQ roadmap covering custody, admin controls, and settlement — or formally disclose the absence of one to every issuer client. A platform without a roadmap is accumulating liability on behalf of its clients.	**Stop onboarding new institutional issuers without disclosing your PQ roadmap status. Every asset issued through your platform inherits your migration debt.**
Oracle / bridge / attestation Chainlink, Wormhole, CCTP, LayerZero	Map every attester key and its on-chain exposure status. Classify signer perimeters by value governed. Treat this as a board-level security item, not an engineering backlog.	Publish a signer-level PQ migration timeline. Begin evaluation of NIST FIPS 204/205 for attester and bridge signing. Notify institutional clients of current exposure posture.	**Stop conflating chain-layer PQ plans with bridge and oracle signer migration. They are different problems with different owners. Your signer perimeter cannot wait for the chain.**
Bank / payment processor Visa, JPMorgan, DTCC, Stripe/Bridge	Separate legacy on-chain settlement exposure from new issuance decisions. Map which on-chain keys are permanently exposed. Define minimum PQ criteria for any new blockchain rail engagement.	Require PQ roadmap disclosure from every blockchain rail used for institutional settlement. Evaluate auditable-private settlement architectures for any new on-chain payment or settlement programme.	**Stop treating post-quantum risk as a future security problem in your blockchain programmes. Migration debt, privacy contamination, and governance burden are accumulating today against assets that never needed to carry them.**

THE NEW-ISSUANCE CONVICTION STATEMENT · APRIL 2026 ONWARDS

After April 2026, every new issuance on a non-PQ-safe blockchain rail is a **knowing decision**. The evidentiary record is complete and public. NIST post-quantum standards were finalized in August 2024. The European Commission mandated national PQC strategies for EU member states by 2026 and quantum-resistant encryption for critical infrastructure by 2030. Google's whitepaper is in the public record as of March 30, 2026, with its authors explicitly stating that the correct planning assumption is a threshold model — meaning no significant notice period before a CRQC exists. The Ethereum Foundation has acknowledged urgency and published a roadmap. Project Eleven and the Solana Foundation have confirmed in live testnet that quantum-safe migration imposes ~90% throughput loss. Cloudflare has already migrated. Android 17 will ship ML-DSA post-quantum signatures natively. The US government has set a 2030–2035 critical infrastructure deadline. The institutional blockchain stack is the only

major financial infrastructure that has not begun. **Fidelity launched FIDD — a new institutional stablecoin on Ethereum mainnet — in February 2026, after all of this was in the public record.** That is the precise definition of a knowing choice. There is no defensible claim of ignorance remaining. Any institution that issues new long-duration stablecoins, tokenized securities, tokenized deposits, or RWAs on quantum-vulnerable rails after this date is making an informed choice to create avoidable migration debt, privacy contamination, and rail-induced liability for assets whose underlying value has nothing to do with blockchain cryptography. That is the board question. Not "when will quantum computers arrive?" — but "can we justify this choice, in writing, to our investors, regulators, and risk committee in 2030, knowing what we know today?"

> ***"There is a right way and a wrong way to issue new value on-chain from here — and the right way is now identifiable."***

SECTION 11

The Institutional Post-Quantum Exposure Framework: *Inventory, Contain, Migrate — What to Do Now*

The three-plane model is the core analytical framework of this report. Every exposure, attack vector, and remediation maps to one of three planes. Understanding which plane your exposure sits in determines the correct response.

	WHAT IT CONTAINS	PRIMARY ATTACK VECTORS
PLANE 01 **Asset Plane** ASSET	• **Token balances** and on-chain asset positions • **User and investor wallets** — any wallet that has transacted exposes its public key • **Staked assets** — ~37M ETH in BLS-signed validator positions • **Bitcoin UTXOs** — ~6.9M BTC in key-exposed addresses • **Tokenized fund shares** — BUIDL, FOBXX, MONY, FYOXX	**On-Spend Attack** ~9 min window on Bitcoin. Fast-clock CRQC required. Solana's 400ms finality narrows this significantly. **At-Rest Attack** No time pressure. Any exposed public key is a permanent target. Ethereum permanently exposes keys on first transaction.
PLANE 02 **Control Plane** CONTROL	• **Admin keys** — mint, burn, freeze, upgrade authority for $200B+ in stablecoins and RWAs • **Governance multisigs** — Security Councils, protocol DAOs, timelock controllers • **Transfer-agent signing** — Securitize keys governing official ownership records • **Bridge attesters** — Wormhole, CCTP, LayerZero signing perimeters • **Oracle signers** — Chainlink price feed authorization keys	**At-Rest Attack (highest priority)** Admin keys permanently on-chain. $200B governed. <15 hours per key on fast-clock CRQC. No social engineering required. This is the institutional-scale threat. **Social Engineering (today)** $285M Drift exploit via multisig social engineering. Under quantum threat, this step is eliminated for exposed key surfaces.

	• **DTC override keys** — master authority for U.S. capital markets tokenized settlement	
PLANE 03 **Privacy Plane** PRIVACY	WHAT IT CONTAINS • **Transaction flows** — every on-chain transfer permanently recorded • **Balances and counterparties** — all observable on public chains • **Treasury strategy** — rebalancing timing, collateral movements, counterparty relationships • **Investor identities** — wallet-to-entity linkages via on-chain analysis • **Settlement patterns** — Visa stablecoin flows permanently visible on Solana	PRIMARY ATTACK VECTORS **Harvest-Now-Decrypt-Later** Data collected in 2026 decrypted in 2031+. Blockchain data is permanent — retroactive privacy failure has no remediation. **On-Setup Attack (Ethereum DAS)** One-time CRQC computation on KZG ceremony creates permanent classical backdoor enabling universal data-availability manipulation.

Where exactly are we exposed?

Build a programme register. Map the dependency stack: tokenization providers, custodians, transfer agents, exchanges, oracles, bridges, settlement rails. Map the crypto primitive register: which signing algorithms and key types underpin each? Build the control-plane key register: which public keys are permanently exposed on-chain, and what value do they govern?

Is the exposure in the asset, control, or privacy plane?

Asset plane: where does the asset live and how is movement authorized? Control plane: who can mint, burn, freeze, upgrade, redeem, attest, settle, or override? Privacy plane: what can the market infer now or retroactively about flows, balances, counterparties, and strategy? Each plane has different urgency and remediation approaches.

Is this legacy exposure or new issuance?

Separate the contain-and-migrate decision from the new-issuance decision. Legacy exposure requires a migration plan and vendor engagement. New issuance requires a different question: which destination architecture eliminates the debt before it is created? Merging these into one programme produces incorrect prioritization.

Do critical vendors and rails have credible PQ roadmaps?

A credible roadmap names the targeted cryptographic standards, supplier migration timeline, client implications, privacy model, and governance path for the full workflow — custody, admin controls, settlement, interoperability, and audit. Anything weaker is posture. The slowest critical-path vendor governs the migration floor.

TABLE 11.1 — NEAR-TERM ACTION PLAN ALIGNED TO NCSC MILESTONES

HORIZON	ACTIONS	NCSC ALIGNMENT
0–30 days	Board mandate; define new-issuance rail policy; begin programme register; identify highest-value control-plane surfaces; assign ownership of PQ programme	Pre-discovery: governance prerequisite
30–90 days	Map dependencies, crypto primitives, control-plane keys, and privacy exposure; begin supplier PQ diligence using the credible-roadmap definition above; identify five most critical-path vendors	Toward 2028 discovery milestone
90–180 days	Harden enterprise perimeter with NIST FIPS 203/204/205 tooling; classify programmes as legacy or new issuance; define migration patterns; begin parallel-rail testing	Early 2028 milestone delivery

HORIZON	ACTIONS	NCSC ALIGNMENT
6–18 months	Run destination-architecture pilots for new issuance; begin highest-priority legacy migrations; board-level PQ reporting cadence; require PQ disclosure from all new and renewing suppliers	Toward 2031 priority-migration milestone

FIVE THINGS TO STOP DOING IMMEDIATELY

	STOP DOING THIS	WHY — AND WHAT TO DO INSTEAD
×	**Issuing new long-duration tokenized assets on quantum-vulnerable rails without a PQ migration plan**	Every new token, fund share, or stablecoin unit issued on a non-PQ-safe rail adds to the migration coordination burden. Stop new issuance on legacy rails and route new programmes to PQ-native infrastructure or to rails with credible and time-bound full-stack PQ roadmaps.
×	**Renewing vendor and supplier contracts without PQ roadmap disclosure requirements**	Tokenization providers, custodians, transfer agents, oracles, and bridges that cannot provide a credible PQ roadmap are adding to your migration critical path. Require PQ disclosure in all new and renewing contracts. Your migration floor is your slowest supplier.
×	**Treating the chain upgrade as sufficient**	Ethereum's base-layer upgrade by 2029 does not migrate your deployed smart contracts, bridge attesters, oracle keys, transfer-agent signing, or custody perimeter. Stop conflating chain-layer PQ plans with full-stack PQ readiness. They are different problems with different owners.
×	**Leaving admin keys and control surfaces permanently exposed on-chain without a rotation or migration plan**	Every day an admin key with upgrade, mint, or freeze authority over a significant balance remains permanently exposed on-chain, it is an at-rest attack surface requiring only compute, not social engineering, to exploit under a CRQC. Identify all exposed control-plane keys and begin rotation planning now.
×	**Treating post-quantum risk as a future security problem rather than a present financial one**	Migration debt, privacy contamination, governance burden, vendor dependence, and market-structure repricing are already accumulating. The board and risk committee question is not "when will quantum computers arrive?" It is "why are we still creating avoidable liabilities for assets that do not need to carry them?"

TEN QUESTIONS TO ASK EVERY CRITICAL VENDOR BEFORE RENEWING OR EXTENDING A CONTRACT

#	QUESTION	WHY IT MATTERS
Q1	What cryptographic signing algorithms underpin your authorization, transaction signing, and key management systems today?	Identifies whether vendor is on secp256k1, Ed25519, or another quantum-vulnerable curve.
Q2	Have you published or will you publish a post-quantum migration roadmap covering your full signing perimeter — not just the chain layer?	"We will migrate when the chain does" is not an answer. The chain migrating does not migrate the vendor's keys.
Q3	Which NIST post-quantum standards (FIPS 203, 204, 205) have you evaluated or begun implementing, and on what timeline?	NIST standards have been final since August 2024. A vendor who has not evaluated them is not on a credible path.
Q4	Which of your public keys are permanently exposed on-chain, what value do they govern, and what is your plan to rotate them?	Identifies admin key exposure at the vendor layer — often the most material institutional control-surface risk.

#	QUESTION	WHY IT MATTERS
Q5	How does your privacy model handle the harvest-now-decrypt-later threat for data recorded on-chain before your PQ migration?	Historical on-chain data is permanent. A vendor who cannot answer this has not addressed privacy durability.
Q6	What is your plan for bridge, oracle, and attestation signing under a post-quantum migration — and what is the timeline?	Bridge and oracle keys are among the highest-value at-rest attack surfaces and are rarely covered in chain-layer PQ roadmaps.
Q7	If the settlement chains you depend on migrate to post-quantum signatures before your infrastructure does, what is your compatibility plan?	A vendor who has no answer faces a potential operational cliff during any chain-layer PQ migration event.
Q8	What is your modeled throughput impact under a post-quantum signature migration, and what is your plan to maintain commercial execution quality?	Live testnet data shows ~90% throughput loss on Solana under quantum-safe signatures. A vendor with no answer to this has not modeled the operational impact.
Q9	What is your auditable privacy model under a post-quantum migration — can you provide selective disclosure to regulators while maintaining confidentiality from market participants?	Auditable privacy is a compliance requirement, not an option. A vendor who cannot provide it under PQ migration is creating regulatory risk.
Q10	Will you contractually commit to completing your post-quantum migration within a specified timeframe, and what is your client communication plan?	A vendor who will not commit to a timeline is not a credible partner for long-duration institutional assets.

VENDOR DILIGENCE SCORECARD — WHAT EACH VENDOR TYPE MUST DISCLOSE BEFORE CONTRACT RENEWAL

VENDOR TYPE	MUST DISCLOSE NOW	RED FLAG ANSWER	PROCUREMENT CONSEQUENCE
Custodian	Key model (HSM type, signing architecture), PQ migration roadmap with timeline, key rotation plan for all on-chain-exposed keys, policy-engine compatibility with NIST FIPS 203/204/205	"We are monitoring the quantum threat" or "We will upgrade when the chain does"	Do not renew long-term agreements without binding PQ roadmap commitment. Begin RFP for PQ-capable alternatives.
Tokenization platform	Admin-control model, upgrade-authority key exposure, transfer-agent signing perimeter, full-workflow migration plan, privacy model under PQ migration	No published workflow-level PQ roadmap; cannot explain what happens to deployed contracts under chain-layer migration	Block new asset issuance through platform until PQ roadmap is disclosed. Every asset issued through an unprotected platform inherits that platform's migration debt.
Stablecoin issuer	Mint/burn/freeze key perimeter, admin key exposure on-chain, interoperability migration plan, reserve-backing continuity under migration, privacy model for institutional flows	"Our chain will upgrade later" — acceptable only if the issuer can specify the end-to-end workflow migration beyond base-layer	Increase institutional dependence on a stablecoin without a full-stack PQ answer only with documented board approval of the residual risk.

VENDOR TYPE	MUST DISCLOSE NOW	RED FLAG ANSWER	PROCUREMENT CONSEQUENCE
Oracle / bridge provider	Signer model (how many signers, which keys, on-chain exposure level), transition path to PQ-safe attestation, timeline, and client migration dependencies	No signer-level PQ plan; conflates chain-layer upgrade with bridge/oracle signer migration	Treat oracle and bridge providers with no signer-level PQ plan as critical-path bottlenecks. They determine your migration floor regardless of your own readiness.
Transfer agent / registry	Signing algorithm for ownership records, upgrade-authority key exposure, investor-record privacy model, compliance with NIST FIPS 205 or equivalent	"Ownership records are off-chain" — irrelevant if the on-chain representation or approval logic uses exposed keys	Any new fund or security issuance requires transfer-agent PQ roadmap as a precondition. Transfer-agent migration failure is a legal and compliance risk, not only a security risk.
Settlement / exchange layer	Hot-wallet signing model and on-chain key exposure, treasury-key PQ plan, settlement-finality model under quantum threat, throughput impact assessment	No throughput impact assessment — Project Eleven confirmed 90% Solana slowdown in live testnet; any exchange that has not modeled this is not credible	For institutional settlement, require PQ throughput impact disclosure before committing volume. A commercially unviable settlement rail after PQ migration is worse than none.

SECTION 12

Post-Quantum Market Infrastructure and Quantum-Safe Tokenization: *What a Credible Destination Architecture Must Have*

TABLE 12.1 — DESTINATION-ARCHITECTURE RUBRIC FOR PQ-SAFE INSTITUTIONAL FINANCE

REQUIREMENT	WHY IT IS NECESSARY	WHAT PARTIAL SOLUTIONS MISS
PQ-safe authorization	New issuance should not embed obvious future cryptographic debt; signing algorithm must be durable for the expected asset life	Wallet-only PQ overlay: hardens enterprise edge but does not fix rail-level authorization or settlement finality
Migration support for legacy assets	Institutions need a path out — vault mechanisms, bridge architecture, re-issuance tooling — not only a clean room for new assets	A PQ-native chain with no migration capability forces complete re-issuance rather than gradual migration
Wallet, custody, and policy integration	Institutions live in control planes: policy engines, custody approvals, compliance gates, and multi-party authorization must be natively integrated	Chain-only PQ upgrade leaves institutional custody workflows unchanged
Auditable privacy	Confidentiality for flows, balances, and counterparties plus selective disclosure for compliance — simultaneously, not traded off	Public rails satisfy neither; hard-privacy rails fail compliance; only auditable-private model with PQ-safe foundations satisfies both
Commercial execution quality	A system that degrades throughput by 30–77% below competitive baselines will not	NIST FN-DSA imposes ~77% TPS loss on Solana, ~31% on Ethereum — commercially unviable for

REQUIREMENT	WHY IT IS NECESSARY	WHAT PARTIAL SOLUTIONS MISS
	win institutional adoption regardless of security properties	high-throughput institutional workflows
Governance quality	Credible, transparent upgrade and policy processes without requiring broad decentralized community consensus for time-sensitive security upgrades	Ethereum's PQ migration challenge — requiring consensus across 10+ client teams — illustrates this fragility
Interoperability	Institutions do not operate in silos; assets must move across custody systems, chains, between DeFi and TradFi environments	A perfectly secure but isolated chain that cannot interoperate with DTCC, JPMorgan's Canton layer, or institutional settlement will not be adopted

SECTION 13

Why Partial Fixes Fail and Why Non-PQ-Safe Privacy Chains Cannot Solve Institutional Post-Quantum Blockchain Risk

TABLE 13.1 — ALTERNATIVES COMPARISON: WHAT EACH APPROACH SOLVES AND WHAT IT LEAVES OPEN

OPTION	WHAT IT SOLVES	WHAT IT LEAVES UNRESOLVED	BEST USE CASE
Wait for underlying chain upgrades	Defers integration burden; leverages chain-team investment	Compounds migration debt during the wait; Ethereum's 2029 covers only base-layer, not contracts, bridges, or L2s; Solana has no disclosed equivalent	Only for tightly contained, low-sensitivity, short-duration legacy exposure
Wallet-only PQ overlay	Hardens enterprise edge and client authorization	Does not address rail-level authorization, settlement finality, or admin-key exposure in smart contracts	Good immediate containment; not a new-issuance answer
Parallel rails	Enables staged migration and operational learning	Adds operational complexity and liquidity fragmentation during transition	Most practical for large institutions with long lead times
Full re-issuance and migration	Eliminates legacy rail dependence once complete	Highest coordination and legal complexity; client consent at scale required	Best for systemically important migrations where completeness is more important than speed
Permissioned containment	Improves control and operational privacy vs. public rails	Not automatically PQ-safe; potential proprietary lock-in; durability depends on underlying cryptography	Useful if genuine migration to PQ-safe architecture is on roadmap with credible timeline
Privacy-only approach (Zcash, Monero model)	Better present-state transaction confidentiality than public-by-default rails	Zcash Sapling trusted setup vulnerable to on-setup quantum attack; Monero Ed25519 quantum-vulnerable; retroactive exposure risk for all historical shielded transactions; no compliance-ready selective disclosure; regulatory friction	Architecturally inadequate for institutional finance requiring compliance, scale, and cryptographic durability

OPTION	WHAT IT SOLVES	WHAT IT LEAVES UNRESOLVED	BEST USE CASE
Phased PQ hardening — wallet-first (Circle Arc model, April 2026)	Opt-in PQ wallet signatures at mainnet (SLH-DSA-SHA2-128s, 7,856 bytes); privacy near-term post-mainnet; validator PQ explicitly deferred to long-term; no published TPS benchmark under PQ load	Validator hardening deferred means the consensus layer remains quantum-vulnerable; new issuers still accumulate migration debt at each phase boundary; 7,856-byte signature choice is 49× larger than EternaX's scheme — throughput implications unquantified publicly; privacy post-mainnet means HNDL exposure from day one of mainnet; the phased approach is more orderly than doing nothing, but each deferred phase is a future migration event for every issuer who builds during the wait	Credible for institutions that need Circle's EVM tooling and are willing to accept phased migration risk; not a day-one full-stack PQ-native answer
PQ-native institution-compatible destination rail	Avoids creating fresh debt on new issuance; integrates PQ-safe authorization, auditable privacy, migration support, and execution quality from inception	Must prove technical and commercial viability; requires institutional-grade governance and interoperability; adoption and partner traction must be demonstrated at scale	Best answer for new long-duration issuance of stablecoins, tokenized funds, tokenized deposits, and RWAs

MARKET CATEGORY DEFINITION · THE CORRECT FRAME FOR THE NEXT INSTITUTIONAL STANDARD

The market category is post-quantum market infrastructure for institutional finance. The real competition is not which legacy chain upgrades later — it is which full-stack quantum-safe tokenization infrastructure is genuinely fit for long-duration institutional value.

The category being created is not post-quantum blockchain. It is not post-quantum security. It is **post-quantum market infrastructure for institutional finance** — a stack combining PQ-native issuance, PQ-safe control planes, auditable privacy, migration rails, institution-grade custody and policy integration, and market-speed execution quality. Issue. Migrate. Custody. Trade. Settle. That full sequence, end to end, under a PQ-safe and auditable-private model. The institution that defines and owns this category wins not because it built a secure chain. It wins because it built the only infrastructure where issuing long-duration institutional value creates no avoidable future liability.

THE QUESTION · ***Does any market participant currently satisfy all seven requirements simultaneously? The answer to that question determines who wins the next institutional issuance decision. Section 15 evaluates the only market participant currently building to answer yes.***

SECTION 15

EternaX: *The Full-Stack Post-Quantum Infrastructure for Institutional Finance*

The requirements established through this report constitute a demanding rubric. Seven requirements. Every one of them necessary. None of them optional for long-duration institutional value. The analysis that follows evaluates each requirement against EternaX's current positioning, with evidence cited and open items disclosed. The conclusion the rubric evidence supports: EternaX is the only market participant currently building to satisfy all seven simultaneously — the full stack of PQ-native issuance, migration infrastructure, custody and policy integration, auditable privacy, and market-speed execution quality, designed from inception rather than retrofitted onto a quantum-vulnerable architecture.

TABLE 15.1 — ETERNAX AGAINST THE FULL-STACK INSTITUTIONAL REQUIREMENT RUBRIC

REQUIREMENT	ETERNAX POSITIONING	EVIDENCED TODAY	REQUIRES DILIGENCE
PQ-safe authorization	Information-theoretic security (not computational hardness); 160-byte signature, 64-byte public key; forgery probability ~1/2^255; 4x+ smaller than next-best NIST standard; pending IACR Journal of Cryptology publication	**Yes — peer-reviewed publication pathway**	Independent validation; peer review completion
Throughput under PQ	~2% TPS loss under PQ migration vs. Solana ~77%, Ethereum ~31%. Protocol-native scheme rather than retrofitted NIST standard. See methodology note in Table 3.2.	**Yes — benchmarked; methodology disclosed**	Production-scale external validation
Migration support	PQ Vault for ETH/EVM assets; PQ Migration Bridge; migration vaults live on testnet	**Yes — vault and bridge live on testnet**	Enterprise integration depth; security review
Wallet, custody, policy integration	PQ-safe wallet live; KYA-ready policy controls; institutional custody integration in development	**Yes — PQ wallet live; 475K+ prediction-market bets on testnet**	Enterprise custody partner traction; policy-engine completeness
Auditable privacy	Privacy layer built on same information-theoretic foundations as authorization — quantum-durable at both layers; selective disclosure for compliance; hidden flow details from market participants; verifiable settlement without broadcasting counterparty or strategy data. EternaX is the only blockchain where harvested transaction data cannot be retroactively decrypted by a quantum computer.	**Yes — architecture specified; privacy design in public documentation and available for institutional review**	Full cryptographic specification published; independent security review
PQ-native issuance	PQ Issuance and Tokenization Rails for stablecoins and RWAs; issue with no migration debt from day one; testnet live, 1M+ transactions processed	**Yes — core product positioning; testnet operational**	Live institutional issuance partnerships; regulatory approvals
Full-stack sequencing	Issue → Migrate → Custody → Trade → Settle; prediction markets live; perpetuals next	**Yes — explicitly stated; testnet validating**	Venue depth and liquidity at scale; institutional traction

On the "Requires Diligence" Items. The rubric table above is intentionally honest — it includes a "Requires Diligence" column rather than claiming every item is fully resolved. Institutions should understand what EternaX is doing about each open item. On peer review completion: the IACR Journal of Cryptology publication by Dr. Chen Feng, Dariia Porechna et al. is in the submission pipeline; independent cryptographic validation is available upon request to institutions conducting diligence. On production-scale throughput validation: testnet has processed 1M+ transactions and 475K+ prediction-

market bets; independent external benchmarking is the appropriate next step and EternaX welcomes it. On enterprise custody partner traction: institutional custody integration is in active development; the architecture is designed from inception for policy-engine and custody-framework compatibility. On live institutional issuance partnerships: EternaX is in active conversations with issuers and regulatory counsel; announcing partnerships before regulatory and technical readiness is complete would itself be a credibility signal in the wrong direction. The "requires diligence" column is transparency, not weakness. It is the column that distinguishes a credible institutional technology claim from a marketing document.

The Four Structural Moats. A rubric match shows EternaX satisfies requirements. The moat analysis shows why that positioning is durable and difficult to replicate.

Moat 01 · Primary Differentiator

Authorization: Information-Theoretic, Post-Assumption

EternaX's cryptographic scheme achieves information-theoretic security — not relying on any computational hardness assumption that could be broken by quantum computing or any future advance. Forgery probability ~1/2^255 is independent of the attacker's computational resources. For a board member or risk committee: this means EternaX's security does not depend on quantum computers being too slow, too expensive, or too near-term. It is secure against any computer, at any speed, with any number of qubits, permanently. Every other post-quantum approach — NIST FIPS 204, 205, 206, Arc's chosen SLH-DSA scheme, Algorand's Falcon — shifts the hard problem to one quantum computers cannot currently solve. That still leaves a residual long-term exposure as algorithms improve. EternaX removes the computational hardness assumption entirely.

`Not computational hardness — computational independence`

Moat 02

Throughput: ~2% TPS Loss vs. 31–90% for Incumbents — and 49× Smaller Signatures Than the Best-Resourced Competitor

Live testnet data from Project Eleven and the Solana Foundation (April 2026) shows ~90% throughput loss on Solana under quantum-resistant signatures. FN-DSA imposes ~31% TPS loss on Ethereum. Circle chose SLH-DSA-SHA2-128s for its Arc blockchain — at 7,856 bytes per signature, that is 122× larger than Ed25519 and 49× larger than EternaX's 160-byte protocol-native scheme. Nic Carter framed the industry's minimum unavoidable cost as a "10× deterioration in signature sizes" under any NIST-compliant approach. EternaX's scheme is 2.5× current — below Carter's stated floor for any NIST-compliant migration. This is not a model: it is a comparison against the specific scheme the most credible institutional blockchain issuer just publicly chose. Competitors cannot adopt PQ authorization without accepting this throughput sacrifice. EternaX's 160-byte integration cannot be replicated by existing chains without a complete protocol redesign — the multi-year coordinated upgrade the Ethereum Foundation's roadmap illustrates, and that Circle's own phased validator deferral acknowledges.

`Live-testnet-confirmed — 49× size advantage vs. Arc's named scheme`

Moat 03

Privacy: PQ-Safe Auditable Privacy — Both Layers, Not Just Signing

Most post-quantum migration discussions focus on the signing layer. EternaX's privacy moat operates at a different level entirely. EternaX's privacy layer is built on the same information-theoretic foundations as its authorization layer — meaning transaction flows, balances, and counterparty relationships on EternaX are private not just from today's adversaries, but from any future adversary regardless of their computational resources. Harvested EternaX transaction data cannot be retroactively decrypted by a quantum computer — because the privacy model does not rest on computational hardness assumptions. Every other blockchain in this report fails this test. Ethereum and Solana are public-by-default. Zcash's Sapling setup is quantum-attackable. Monero uses Ed25519. Circle's Arc defers privacy to a post-mainnet roadmap phase. Once institutional workflows are built on an auditable-private, information-theoretically durable privacy model, switching cost is high because the compliance and regulatory architecture is co-designed with the privacy model. That is the most durable form of institutional lock-in: security that does not expire, compliance that is built in, and a migration path out that is as expensive as the one they are trying to avoid.

`PQ-safe at both layers — authorization AND privacy`

Moat 04

Systems: Full Stack — Issuance + Migration + Policy + Venues

No other market participant is attempting to solve the complete institutional workflow sequence simultaneously: PQ-native issuance → migration vaults → custody and policy controls → market venues → settlement. Each individual layer has existing participants. The full integrated stack, designed for PQ-native institutional finance from inception, does not. The moats compound: a competitor who adds PQ signatures still lacks throughput advantage and auditable privacy; one who improves throughput still lacks information-theoretic authorization; one who adds privacy still lacks migration rails and institutional venue infrastructure. Retrofitting the full stack takes longer than building it correctly from scratch — precisely as the Ethereum Foundation's multi-year, multi-fork roadmap illustrates, and as Circle's decision to defer validator hardening to a long-term phase confirms. The category winner is not the chain that migrates latest. It is the infrastructure that never needed to migrate.

`The category winner never needed to migrate`

The market EternaX competes in has two distinct components: the migration market (assets already on quantum-vulnerable rails that will require re-platforming over the NCSC 2028–2035 window), and the new-issuance market (every dollar of long-duration institutional value that will be tokenized from here, which faces a binary choice between legacy vulnerable rails and PQ-native infrastructure). The new-issuance market is the primary opportunity — it requires no migration coordination, no counterparty consent, and no legacy smart contract replacement. It requires only a decision at the moment of issuance.

$3.1T

ON-CHAIN VALUE TODAY (STABLECOINS + RWAS). EVERY DOLLAR CURRENTLY ON QUANTUM-VULNERABLE RAILS. THE MIGRATION ADDRESSABLE MARKET OVER THE NCSC 2028–2035 PLANNING HORIZON.

$72T

PROJECTED ON-CHAIN BY 2028 ($68T TOKENIZED RWAS + $4T STABLECOINS). EVERY DOLLAR OF NEW LONG-DURATION INSTITUTIONAL ISSUANCE FROM HERE IS A DIRECT CHOICE: MIGRATE-LATER LIABILITY OR ZERO-DEBT PQ-NATIVE ISSUANCE.

EternaX's revenue architecture follows the same funnel as its product stack: Issue → Migrate → Custody → Trade → Settle. Each layer generates a distinct revenue stream — venue fees on market activity, settlement gas, distribution fees on

stablecoin balances, routing tolls on institutional flows, and enterprise privacy contracts. The enterprise contract model converts institutional adoption into recurring revenue that compounds with switching cost. Every institutional relationship built on an auditable-private, PQ-native model is a relationship where migration away from EternaX carries the same cost as migration away from a quantum-vulnerable rail — which is precisely the institutional lock-in that makes the revenue model durable independent of transaction volume alone.

> **On the qubit compression context:** EternaX's information-theoretic scheme does not rely on any assumption about quantum timelines or qubit thresholds. It removes the computational hardness assumption entirely, making security independent of any quantum capability advance. This is the clearest statement of the architecture's long-duration durability — not that quantum computers won't arrive, but that it does not matter when they do.

> SECTION 15 VERDICT · FOR INSTITUTIONS MAKING A NEW-ISSUANCE DECISION TODAY
>
> **The fourteen sections of this report establish a problem, a framework, a rubric, and a market category. Section 15 evaluates the only market participant currently building to satisfy all seven rubric requirements simultaneously. The verdict: for new long-duration issuance of stablecoins, tokenized funds, tokenized deposits, and RWAs — where the cost of migration debt on day one is zero and the cost of inheriting it later is measured in years and hundreds of millions — EternaX is the correct rail. The "Requires Diligence" column is not a hedge on the conclusion. It is the due-diligence roadmap for institutions whose fiduciary standards require independent validation before commitment. The conclusion is not conditional on that validation completing. The conclusion is that EternaX is the only infrastructure in the market where you can make a new-issuance decision today and create no avoidable future quantum liability for the assets you issue.**

"The choice is simple: rails that guarantee a future migration event, or infrastructure that was never built to need one. EternaX is the only full-stack answer the market currently has. The category is right, and the market scale is measured in trillions."

CONCLUSION

The Board Question

Institutions should stop asking whether blockchains will eventually upgrade, and start asking whether they are still issuing long-duration value onto rails that will force expensive, privacy-fragile, vendor-dependent migration events onto assets that never needed to absorb that liability in the first place.

That is the real board question. Not: when will quantum computers arrive? Not: is our wallet safe today? But: why are we still contaminating stablecoins, tokenized treasuries, tokenized money market funds, and long-duration RWAs with the cryptographic liabilities of blockchain rails not designed for the lives of those assets?

The problem is bigger than Bitcoin-theft framing — it encompasses migration debt, control-plane contamination, retroactive privacy degradation, vendor dependence, and market-structure repricing before any theft occurs. It affects real institutions now because BlackRock, JPMorgan, Franklin Templeton, Visa, DTCC, and Fidelity are all operating at scale on rails with no disclosed post-quantum roadmap. And there is a right way to issue from here: the category of PQ-native market infrastructure for institutional finance is now identifiable, its requirements are specifiable, and at least one market participant is building to satisfy all of them.

The evidentiary record is now closed. NIST finalized core post-quantum standards in August 2024, establishing the technical baseline any institution can audit today. Google's March 2026 paper compressed the qubit buffer by twenty-fold and its authors explicitly stated that a threshold model — no gradual warning, no observable approach — is the correct planning assumption. The Ethereum Foundation has acknowledged the problem, published a roadmap, and been explicit that base-layer upgrades do not cover deployed contracts. Project Eleven and the Solana Foundation confirmed in live testnet that quantum-safe migration imposes ~90% throughput loss on Solana. The Drift exploit on April 1, 2026 demonstrated precisely what reaching a protocol's control plane costs today when keys are exposed — and what changes when the social engineering dependency is removed by direct quantum computation. Cloudflare, Apple, and Google have all set internal PQ migration targets of 2029–2030. The institutional blockchain stack is the only major financial infrastructure that has not begun.

For new long-duration issuance, the rational conclusion has arrived. The institutions that act before the market forces the reckoning will be the architects of the next institutional standard. Those that defer will be the subjects of an expensive, public, and entirely avoidable migration.

> *"The only serious remaining question is not whether institutions should address this. It is whether they will be positioned as the architects of the next institutional standard — or as the subjects of an expensive and avoidable migration."*

NEXT STEP

Discuss Your Institution's Post-Quantum Exposure with EternaX

For institutional diligence on post-quantum financial infrastructure, stablecoin architecture, tokenized finance risk, cryptographic migration debt, or EternaX's PQ-native issuance and migration rails.

PAARRTHHH BIRLA · CO-FOUNDER

DARIIA PORECHNA · CO-FOUNDER

RELATED ETERNAX RESEARCH

EternaX Post-Quantum Research Series

This report is the second in the EternaX Post-Quantum Research Series. The first report, published in March 2026, established the foundational post-quantum threat case across 27 named institutions and nine chains, introduced the concept of cryptographic migration debt, and identified nine open 2026 architecture decisions still available to institutions before lock-in. This report extends that work by developing the enterprise-first exposure framework, the enterprise-to-rail trace methodology, the full migration-debt taxonomy, and the institutional post-quantum decision framework.

ETERNAX RESEARCH SERIES — POST-QUANTUM FINANCIAL INFRASTRUCTURE

REPORT	TITLE AND FOCUS	KEY CLAIMS	LINK
Q1 2026	**Already Broken: The Post-Quantum Threat to Stablecoins, Tokenized Finance, Privacy Chains, and Cryptographic Migration Debt** — 27 named institutions, nine chains, nine chains verdicted, $57B–$135B first-order exposure, nine open 2026 architecture decisions	27 institutions. 0 PQ plans. 9 open decisions. Migration debt introduced as a named category.	Read Q1 2026 →
Q2 2026	**Cryptographic Migration Debt: The Post-Quantum Exposure Framework for Institutional Digital Asset Programmes** — Enterprise-to-rail trace for BUIDL, Visa, and DTCC; full migration-debt taxonomy; institutional post-quantum exposure framework; quantum-safe tokenization rubric; EternaX four-moat case	9 programmes. 0 PQ roadmaps. Enterprise-first framework. Full-stack solution category named.	This report

For questions, institutional diligence, or partnership enquiries related to either report, contact info@eternax.ai. For the EternaX technical architecture and product documentation, visit eternax.ai.

FREQUENTLY ASKED QUESTIONS

19 Questions, Answered: *Post-Quantum Risk in Institutional Digital Asset Programmes*

What is cryptographic migration debt in the context of post-quantum risk?

Cryptographic migration debt is the compounding set of operational, governance, liquidity, privacy, and reputational costs that an institution incurs when it issues long-duration value on quantum-vulnerable blockchain rails. Unlike traditional technical debt, cryptographic migration debt accrues at issuance time — not at break time — and compounds with every new counterparty, blockchain deployment, DeFi integration, and client relationship. For a $2.85 billion fund like BlackRock's BUIDL, operating across nine blockchains with hundreds of DeFi integrations, the migration coordination debt is already substantial — and growing with every successful expansion. **The EternaX answer:** EternaX is designed so that new issuance on its rails creates zero migration debt from the first transaction. Its protocol-native PQ scheme, PQ-safe privacy layer, and full-stack architecture mean there is no future retrofit event to coordinate. Institutions that issue on EternaX today do not inherit the liability they are trying to avoid.

What did Google's March 2026 quantum whitepaper actually claim about crypto?

Google Quantum AI's March 30, 2026 whitepaper — co-authored with the Ethereum Foundation and Stanford — demonstrated that breaking secp256k1 (the curve securing Bitcoin and Ethereum) could be done with fewer than 500,000 physical qubits on a superconducting architecture, a roughly 20-fold reduction from prior estimates of ~9 million. Google estimated execution time in minutes. The paper also showed that on-spend attacks carry a ~41% success probability within Bitcoin's 10-minute block window. Critically, Google's Section VI.D explicitly extended the analysis to Ethereum's smart contracts, stablecoins, tokenized RWAs, and Proof-of-Stake validators. Google called the expected emergence of CRQCs "a singular discontinuity in the history of digital security."

Why is post-quantum risk particularly severe for stablecoins and tokenized RWAs?

Stablecoins and tokenized RWAs derive their value from off-chain sources — dollar reserves, U.S. Treasury securities, bank deposits, legal claims. The blockchain is merely the rail. A quantum attack on that rail contaminates otherwise clean financial claims with an avoidable cryptographic liability those assets never needed to carry. Google's paper specifically estimated that ~$200 billion in stablecoins and tokenized assets on Ethereum depends on admin keys already permanently exposed on-chain — keys that control minting authority for major stablecoins. A successful attack could allow arbitrary token creation entirely decoupled from the underlying reserve. **The EternaX answer:** Stablecoins and RWAs issued on EternaX carry no quantum liability from inception. EternaX's information-theoretic authorization means minting authority cannot be forged regardless of quantum capability. Its PQ-safe privacy layer means the flows, balances, and counterparty relationships of issued assets remain private permanently. The underlying value — reserves, legal claims, sovereign credit — stays clean because the rail was designed not to contaminate it.

What is the difference between post-quantum risk on Ethereum versus Solana?

Both chains use quantum-vulnerable elliptic curve cryptography, but the risk profiles differ structurally. Ethereum permanently exposes public keys on first transaction, has five distinct vulnerability classes, and carries ~$200 billion in stablecoin and RWA admin-key exposure. Modeled TPS loss under FN-DSA: ~31%. Solana uses Ed25519, also quantum-vulnerable. Solana's ~400ms finality provides structural protection against on-spend attacks specifically, but zero protection against at-rest attacks on exposed admin keys and governance signers — as demonstrated by the $285 million Drift exploit. Solana's live testnet (Project Eleven / Solana Foundation, April 2026) confirmed ~90% throughput loss under quantum-safe signatures — commercially prohibitive on the current architecture.

What is the harvest-now-decrypt-later threat to institutional blockchain operations?

The harvest-now-decrypt-later (HNDL) threat involves adversaries collecting and storing blockchain data today, with the intention of decrypting it retroactively once quantum capabilities mature. For institutional blockchain operations, on-chain transactions conducted today — settlement flows, collateral movements, counterparty interactions — are being permanently recorded on public ledgers under cryptographic assumptions that may not hold in 2031 or 2033. Since blockchain data is permanent and irrevocable, there is no remediation available once the data is on-chain. An adversary who stores a treasury desk's 2026 on-chain activity and decrypts it in 2032 has effectively time-travelled to observe that institution's strategic positions and counterparty relationships.
The EternaX answer: EternaX's privacy layer is built on information-theoretic foundations — the same ones underpinning its authorization scheme. This means EternaX transaction data cannot be retroactively decrypted by a quantum computer, because the privacy model does not rest on computational hardness assumptions that quantum computing can break. Harvesting EternaX transaction data today yields nothing that a future quantum computer can unlock. This is the only architecture where the HNDL threat is structurally neutralized — not mitigated, neutralized.

Does the Ethereum Foundation's post-quantum roadmap address the institutional tokenized asset stack?

The Ethereum Foundation's roadmap targets base-layer protocol upgrades by 2029 through four sequential hard forks. However, the Foundation explicitly acknowledges that "full execution-layer migration taking additional years beyond that." More critically for institutions: the base-layer upgrade does not automatically fix the thousands of smart contracts already deployed on Ethereum. Each protocol, bridge, and Layer 2 network must independently upgrade its own code and rotate its own keys. No single entity controls or can coordinate that process. BlackRock's BUIDL smart contracts, JPMorgan's MONY token logic, and Fidelity's FYOXX smart contracts each require independent upgrades — entirely separate from whatever Ethereum's protocol team does at the base layer.

What makes EternaX's post-quantum approach structurally different from applying NIST post-quantum standards to existing chains?

Two fundamental differences. First, EternaX uses an information-theoretic security model rather than a computational-hardness security model. NIST post-quantum standards shift the hard problem to one quantum computers currently cannot solve — but security still depends on a mathematical assumption about computational difficulty. EternaX's scheme achieves security that is independent of the attacker's computational resources entirely. Second, EternaX's PQ scheme is protocol-native rather than retrofitted, resulting in ~2% modeled TPS loss versus ~31–90% for existing chains. A chain retrofitting PQ authorization cannot achieve the same throughput efficiency as one designed with PQ-native authorization from inception.

What is auditable privacy and why does it matter for institutional finance?

Auditable privacy is a privacy model providing cryptographic confidentiality for transaction flows, balances, and counterparty identities to market participants — while simultaneously providing selective disclosure capability to regulators, auditors, and compliance functions. It is architecturally distinct from both public-by-default blockchains (which provide transparency to everyone simultaneously) and hard-privacy blockchains (which provide confidentiality but lack compliance-ready disclosure mechanisms). For institutional finance, it is a market-structure requirement: treasury desks and fund managers need counterparty and strategy confidentiality from market participants, but must simultaneously satisfy regulatory reporting obligations and audit requirements. **The EternaX answer:** EternaX implements auditable privacy with PQ-safe foundations — meaning the privacy is not only compliant and institutionally appropriate, it is also quantum-durable. An institution running on EternaX gets hidden flows, selective disclosure for compliance, and the assurance that neither today's adversaries nor future quantum computers can reconstruct the transaction record without authorized disclosure. This combination — compliant, auditable, and information-theoretically private — does not exist on any other institutional blockchain infrastructure today.

Which institutions have disclosed post-quantum migration roadmaps for their tokenized asset programmes?

As of April 2026, none of the nine named institutional programmes examined in this report have disclosed an end-to-end post-quantum cryptographic roadmap covering custody, admin controls, settlement mechanics, interoperability, and audit. The Ethereum Foundation has published a base-layer protocol roadmap targeting 2029, but this does not cover deployed smart contracts or the institutional tokenization stack. Chains including Algorand, XRPL, and Solana have made early experimental PQ deployments at various layers, but none have completed an end-to-end institutional migration. Circle's Arc has published a phased PQ roadmap with wallet signatures at mainnet and validator hardening deferred to long-term. **The EternaX answer:** EternaX does not require a migration roadmap for new issuance — because new issuance on EternaX creates no migration debt to begin with. The distinction is fundamental: every other chain is building a roadmap to eventually reach quantum safety. EternaX starts there. For institutions whose issuance decision is in front of them today, EternaX is the only infrastructure where the roadmap question for new programmes is already resolved.

What should an institution do in the next 30 days about post-quantum risk?

Three immediate actions: First, establish a board mandate defining post-quantum risk as a material programme risk with assigned ownership — this governance prerequisite must exist before any technical work is prioritized correctly. Second, define a new-issuance rail policy specifying what cryptographic criteria any new tokenized asset programme must satisfy before issuance proceeds; this decision is entirely in the institution's control and requires no technical migration work. Third, begin a programme register identifying every digital asset product, workflow, and infrastructure touchpoint, mapped to the underlying signing algorithms, admin key locations, and third-party dependencies — the prerequisite for all subsequent migration planning. **The EternaX answer for new issuance:** If a new stablecoin, tokenized fund, tokenized deposit, or RWA programme is in the decision pipeline, contact EternaX before architecture lock-in. The cost of evaluating PQ-native issuance infrastructure today is a fraction of the coordination cost of migrating an established programme later. EternaX's team can provide institutional diligence materials, technical architecture documentation, and a comparison of the seven-requirement rubric against any alternative architecture under consideration. Contact: paarrthhh.b@eternax.ai or dariia.p@eternax.ai.

What is the quantum threat to Bitcoin specifically?

Post-quantum Bitcoin risk has three distinct exposure types. First, at-rest attacks: approximately 6.9 million BTC are in addresses where the public key is permanently on-chain — including P2PK addresses from the Satoshi era (~1.7M BTC), reused addresses, and all Taproot addresses. A CRQC can derive the private key from any of these with no time pressure. Second, on-spend attacks: Google modeled ~9 minutes to derive a secp256k1 private key, giving ~41% theft probability within Bitcoin's 10-minute block window. Third, Bitcoin has no coordinated PQ migration plan. BIP-360 was merged into the BIP repository in February 2026 but has no confirmed activation. Migration requires every wallet, exchange, custodian, and user to voluntarily upgrade — with no central authority to coordinate it.

What is blockchain rail risk and why does it matter for stablecoins and tokenized securities?

Blockchain rail risk refers to the cryptographic and operational liabilities that a blockchain network introduces to any asset issued on it — liabilities that are separate from the asset's own credit quality, legal structure, or underlying value. For native cryptoassets, rail risk is intrinsic. For stablecoins backed by dollar reserves, tokenized securities backed by U.S. Treasuries, or tokenized deposits backed by banking liabilities, blockchain rail risk is an imported liability. Those assets should not carry quantum-vulnerability risk, migration debt, control-plane fragility, or privacy contamination from their blockchain rail — yet under current infrastructure choices, they do.

What is admin key vulnerability in Ethereum and why is it the institutional number?

Admin key vulnerability in Ethereum refers to smart contracts whose administrative control keys — mint, burn, freeze, pause, upgrade — are permanently exposed on-chain. Google's March 2026 whitepaper identified at least 70 of the top 500 contracts by ETH balance with admin keys on-chain, holding ~2.5 million ETH crackable in under 15 hours. More important for institutions is the $200 billion figure: Google estimated that ~$200 billion in stablecoins and tokenized RWAs on Ethereum are governed by these admin-vulnerable keys. This is the institutional control-surface number, not the end-user wallet number. A successful at-rest attack on a stablecoin issuer's mint authority key could enable unlimited token creation completely decoupled from the underlying reserve.

What is post-quantum risk for tokenized securities?

Post-quantum risk for tokenized securities has four layers. First, the signing layer: ECDSA and Ed25519 signatures — both quantum-vulnerable. Second, the transfer-agent layer: Securitize's signing keys governing the official ownership record for BUIDL and FOBXX are at-rest attack surfaces. Third, the settlement layer: DTCC's DTC override keys and participant wallet registrations. Fourth, the privacy layer: investor identities, holdings, and transaction histories on public blockchains are subject to harvest-now-decrypt-later exposure. Quantum-safe tokenization of securities requires all four layers to be addressed simultaneously.

What is post-quantum risk for tokenized deposits?

Tokenized deposits — bank liabilities issued as blockchain tokens, such as JPMorgan's JPMD — face post-quantum risk concentrated in three places: admin key governance over the token's minting and burning authority; the signing infrastructure of the bank's digital asset custody and settlement operations; and the blockchain rail's cryptographic durability for the expected life of the deposit instrument. A tokenized deposit is a bank product. It should not carry the cryptographic migration debt and control-plane fragility of a blockchain rail not designed for the 5–10 year horizon of an institutional banking product.

What is blockchain privacy durability and why does it matter for institutional on-chain finance?

Blockchain privacy durability refers to the long-term cryptographic soundness of a blockchain's privacy model under a realistic adversary that includes quantum capabilities. Most blockchain privacy today is computationally secure — private only against adversaries without quantum computers. For institutional on-chain finance, blockchain privacy durability matters because on-chain data is permanent. Transaction flows, balances, counterparty relationships, and treasury movements recorded today are permanently subject to future decryption as quantum capabilities improve. An institution whose Q3 2026 treasury operations are on-chain on a non-durable-privacy rail is permanently exposed to harvest-now-decrypt-later — regardless of whether quantum computers arrive in 2030 or 2035. **The EternaX answer:** EternaX is the only blockchain with information-theoretically durable privacy — meaning EternaX transaction data is private not because quantum computers are too slow today, but because the privacy model does not depend on any computational hardness assumption that quantum computing could ever break. This applies to both new transactions and — critically — to any already-recorded transaction data. For institutional programmes where on-chain transaction confidentiality must remain permanent regardless of future computational advances, EternaX is the only infrastructure that satisfies this requirement architecturally rather than conditionally.

What is quantum-safe tokenization and what does it require?

Quantum-safe tokenization refers to the issuance and lifecycle management of tokenized assets on blockchain infrastructure whose authorization model, control-plane governance, privacy architecture, and settlement mechanics are durable against CRQCs. It requires seven simultaneous properties: PQ-safe signing algorithms; admin key governance that does not permanently expose control-surface public keys; a migration path for legacy assets; auditable privacy for institutional transaction flows; commercial execution quality at institutional scale; institution-grade custody and policy integration; and interoperability with regulated financial infrastructure. A chain that satisfies three or four of these properties but not all seven is not a quantum-safe tokenization destination for long-duration institutional assets. **The EternaX answer:** EternaX is designed to satisfy all seven requirements simultaneously — the only infrastructure currently positioning to do so. Critically, EternaX satisfies both the authorization requirement (information-theoretic security, not computational hardness) and the privacy requirement (PQ-safe privacy layer built on the same information-theoretic foundations). This dual-layer quantum safety — authorization AND privacy — is what separates quantum-safe tokenization from quantum-safer tokenization. For the full evaluation against all seven requirements, see Table 15.1 of this report.

What is PQ-native issuance and why is it different from migrating an existing programme?

PQ-native issuance means issuing a stablecoin, tokenized fund, tokenized deposit, or RWA on blockchain infrastructure whose post-quantum security properties are built into the protocol from inception — not retrofitted. The distinction matters for three reasons. First, cost: migrating an established programme is orders of magnitude more expensive than issuing PQ-native from day one. Second, quality: a chain designed PQ-native from inception achieves ~2% TPS loss, while chains retrofitting NIST standards face 31–90% TPS loss. Third, liability: every day an existing programme operates on vulnerable rails, it deepens its migration coordination debt, privacy debt, and governance debt. PQ-native issuance is the only path that creates zero migration debt from the first transaction. **The EternaX answer:** EternaX is the PQ-native issuance infrastructure. Issue a stablecoin on EternaX and it inherits no quantum liability — not at the authorization layer (information-theoretic security, not computational hardness) and not at the privacy layer (PQ-safe foundations, meaning transaction data cannot be retroactively decrypted by any quantum computer). The day-one issuance decision on EternaX is the decision that eliminates the entire future migration event. Contact paarrthhh.b@eternax.ai or dariia.p@eternax.ai to discuss your institution's new-issuance architecture.

What is the institutional post-quantum exposure framework and how should an institution apply it?

The institutional post-quantum exposure framework is a structured methodology for mapping, prioritizing, and remediating post-quantum risk across an institution's digital asset programmes. Three phases: Inventory — map every digital asset product and infrastructure touchpoint to its underlying signing algorithms, admin key locations, third-party dependencies, and privacy surface. Contain — harden the highest-value control-plane surfaces using NIST FIPS 203/204/205 tooling; define a new-issuance rail policy; require PQ roadmap disclosure from critical-path vendors. Migrate — for legacy exposure, build a coordinated migration plan aligned to NCSC's 2028 and 2031 milestones; for new issuance, evaluate PQ-native destination architectures against the seven-requirement rubric in Section 12 of this report. The framework requires board-level ownership and a dedicated PQ risk officer or working group. **The EternaX answer for new issuance:** When the framework reaches the new-issuance evaluation — the question of which destination architecture eliminates the debt before it is created — EternaX is the answer this framework was designed to reach. The seven-requirement rubric in Section 12 maps directly to EternaX's full-stack design. No other market participant currently satisfies all seven requirements simultaneously.

Is EternaX's privacy layer post-quantum safe — and how does it differ from other blockchains claiming privacy?

Yes. EternaX's privacy layer is post-quantum safe, and this is a structurally different property from PQ-safe authorization. Most post-quantum discussions focus on replacing ECDSA/Ed25519 signatures with quantum-resistant alternatives. This addresses who can authorize asset movement. It does not address what adversaries can observe and decode from the permanent on-chain record — which is the privacy threat. EternaX's privacy model is built on the same information-theoretic foundations as its authorization scheme. This means EternaX transaction data — flows, balances, counterparty relationships — is private not just from today's adversaries but from any future adversary regardless of computational resources. Harvested EternaX transaction data yields nothing that a quantum computer can unlock. Compare this to every other blockchain: Ethereum and Solana are public-by-default (no privacy at either layer). Zcash's Sapling trusted setup is itself vulnerable to an on-setup quantum attack, retroactively compromising all shielded transactions. Monero uses Ed25519 ring signatures — quantum-vulnerable. Circle's Arc has deferred privacy to a post-mainnet roadmap phase, meaning Arc issuers accumulate HNDL exposure from day one of mainnet. EternaX is the only blockchain where both the authorization layer and the privacy layer are quantum-durable. For institutions whose transaction confidentiality is a fiduciary requirement — not just a feature — this distinction is not optional.

How can my institution issue a stablecoin or tokenized RWA with zero post-quantum liability from day one?

The answer is EternaX. The path is: issue on a PQ-native rail with PQ-safe privacy foundations, rather than issuing on quantum-vulnerable infrastructure and creating a migration event you will have to manage later. What zero quantum liability from day one means in practice: your minting authority cannot be forged by a quantum computer because EternaX's authorization scheme is information-theoretically secure, not reliant on computational hardness. Your transaction history cannot be retroactively decrypted because EternaX's privacy layer is built on the same information-theoretic foundations — harvested data yields nothing. Your programme will not require a multi-year coordinated migration when the market reprices quantum-vulnerable rails. The cost of new issuance on EternaX is the same as the cost of new issuance on Ethereum or Solana — the difference is that one creates zero migration debt and the other creates compounding liability that grows with every new counterparty, DeFi integration, and client relationship you add. To discuss your institution's new issuance architecture and diligence EternaX against your specific requirements, contact Paarrthhh Birla (paarrthhh.b@eternax.ai) or Dariia Porechna (dariia.p@eternax.ai).

About the Authors

EternaX Labs | Post-Quantum Financial Infrastructure

Dariia Porechna

CO-FOUNDER

Cryptographer and distributed systems architect. Former Head of Protocol at Subspace. Former Research Engineer at Wolfram|Alpha.

LinkedIn · X

Paarrthhh Birla

CO-FOUNDER

Former VP, Growth Office at Polygon. Former Head of Partnerships at Subspace Protocol. Former digital-assets strategy advisor at EYP. MBA, CPA.

LinkedIn · X

Dr. Chen Feng

CHIEF SCIENTIST

Associate Professor, University of British Columbia. PhD, University of Toronto. 100+ peer-reviewed papers across quantum communications, blockchain, and TEE privacy.

LinkedIn · Google Scholar

Contact

Institutional Inquiries

For institutional inquiries regarding post-quantum financial infrastructure, stablecoin post-quantum architecture, tokenized finance post-quantum risk, privacy-chain post-quantum risk, cryptographic migration debt, pre-upgrade time-at-risk, or EternaX post-quantum infrastructure.

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

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

SOURCES

Primary Sources and Citations

[1] Google Quantum AI. "Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations." Babbush, Zalcman, Gidney et al. (Google Quantum AI), Drake (Ethereum Foundation), Boneh (Stanford). March 30, 2026. quantumai.google/static/site-assets/downloads/ cryptocurrency-whitepaper.pdf · research.google/blog/ safeguarding-cryptocurrency-by-disclosing-quantum-vulnerabilities-responsibly

[2] Oratomic/Caltech. "Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits." Cain, Xu, King, Picard, Levine, Endres, Preskill, Huang, Bluvstein. arXiv:2603.28627. March 30, 2026. arxiv. org/abs/2603.28627

[3] Ethereum Foundation. pq.ethereum.org — Post-Quantum Ethereum Research Hub. Launched March 24, 2026. Four-fork roadmap (I, J, L, M) targeting 2029 base-layer upgrade; full execution-layer migration beyond 2029. EF statement: "The work must begin well before the threat arrives."

[4] NIST. FIPS 203 (ML-KEM), 204 (ML-DSA), 205 (SLH-DSA). August 13, 2024. csrc.nist.gov

[5] NCSC. "Timelines for migration to post-quantum cryptography." 2028/2031/2035 enterprise milestones. ncsc.gov.uk/guidance/pqc-migration-timelines

[5a] European Commission / EU Member States. Coordinated PQC transition roadmap, 2025–2026. Requires national PQC strategies by 2026; quantum-resistant encryption for critical infrastructure by 2030. European Union Agency for Cybersecurity (ENISA) coordinating implementation.

[5b] Google / Android. Android 17 to ship ML-DSA (NIST FIPS 204) post-quantum digital signature protection natively. Confirmed April 2026. Represents >3 billion devices adopting PQ signatures by default before most institutional blockchain infrastructure has a disclosed migration roadmap.

[6] BlackRock/Securitize. BUIDL fund: $2.85B AUM (2026); nine chains; $100M+ cumulative dividends (Dec 29, 2025). prnewswire.com; wormhole.com/blog

[7] J.P. Morgan Asset Management. "JPMorgan Launches First Tokenized Money Market Fund (MONY) on Ethereum. " December 15, 2025. am.jpmorgan.com

[8] Digital Asset / Kinexys. "JPM Coin (JPMD) natively to Canton Network." January 7, 2026. prnewswire. com

[9] DTCC/DTC. SEC No-Action Letter (December 11, 2025); Canton Network partnership (December 2025). sec. gov/files/tm/no-action/dtc-nal-121125.pdf; dtcc.com

[10] Visa. "Visa Launches Stablecoin Settlement in the United States." December 16, 2025. usa.visa.com

[11] WisdomTree. "WisdomTree Expands Tokenization Ecosystem to Solana." January 2026. ir.wisdomtree.com

[12] Fidelity. Fidelity Treasury Digital Fund (FYOXX). Mid-2025 launch on Ethereum. coindesk.com (March 22, 2025 filing)

[13] Franklin Templeton. FOBXX/Benji: SEC prospectus; Canton Network expansion (November 2025). franklintempleton.com/FOBXX

[14] Drift Protocol. $285–286M exploit, April 1, 2026. DPRK attribution (Elliptic, TRM Labs). Durable nonce social engineering. elliptic.co; trmlabs.com; coindesk.com (April 2, 2026)

[15] Project Eleven / Solana Foundation. Live testnet: quantum-resistant signatures 20–40× larger than Ed25519; Solana network ~90% slower under quantum-safe cryptography. Pruden: "In Solana, 100% of the network is vulnerable. A quantum computer could pick any wallet and immediately start trying to recover the private key." CoinDesk, April 4, 2026. (Source: Margaux Nijkerk, CoinDesk)

[16] Circle / Arc. "Arc's Quantum-Resistant Design and Roadmap." arc.network/blog, April 3, 2026. SLH-DSA-SHA2-128s (7,856 bytes) chosen for wallet signatures at mainnet; validator PQ deferred to long-term phase; privacy near-term post-mainnet; opt-in approach; no published TPS benchmark under PQ load. CoinDesk coverage: April 6, 2026.

[17] Circle Research. "How Blockchains Are Preparing for Q-Day." circle.com/blog, January 2026. Signature size comparison table: ECDSA 65B → Falcon 666B → ML-DSA 2,420B → SLH-DSA-SHA2-128s 7,856B. Quote: "Active addresses that have already signed transactions must migrate before Q-Day because their public keys have been exposed."

[18] Nic Carter, Castle Island Ventures. Bankless Podcast, April 2026. Quotes cited: no-notice-period argument; Manhattan Project / 1940 framing; Solana "rebuild everything from scratch"; Cloudflare migration completion; Bitcoin governance assessment; signature size floor ("minimum 10× deterioration").

[19] Algorand Foundation. First major L1 mainnet Falcon-1024 transaction, November 3, 2025. State proofs PQ-secured; core accounts still Ed25519; opt-in CLI tool. Cited in Google Quantum AI whitepaper (March 30, 2026) as real-world PQC deployment example.

[20] Brian Armstrong, CEO Coinbase. Public statement, April 6, 2026: personal engagement on quantum threat. No PQ roadmap disclosed for Coinbase custody, exchange, or Base L2.

[21] Fidelity Digital Assets, NA. Fidelity Digital Dollar (FIDD). Launched February 4, 2026. 1:1 USD-backed stablecoin; backed by cash, U.S. Treasurys, or other liquid assets; issued by Fidelity Digital Assets, National Association (subsidiary of Fidelity Investments); available to retail and institutional investors; purchasable/redeemable at $1; transferable to any Ethereum mainnet address; daily circulating supply and reserve NAV disclosure. Source: fidelitydigitalassets.com/stablecoin. No post-quantum migration roadmap disclosed as of April 2026.

Methodology Note: TPS loss figures for Solana (~77%), Sui (~69%), and Ethereum (~31%) use FN-DSA (NIST FIPS 206/Falcon) as the PQ signature replacement. EternaX (~2%) reflects its own protocol-native 160-byte PQ scheme. Not equivalent-methodology comparisons — do not cite without this note.

Disclaimer: Not investment advice. EternaX Labs has a direct commercial interest in the conclusions of this report. All primary source citations are individually verified. Data current as of April 2026. Readers should conduct independent diligence on all claims before making any institutional decision.

---

eternaX

Quantum-safe Settlement at Market Speed

GitHub YouTube Telegram X (Twitter) LinkedIn