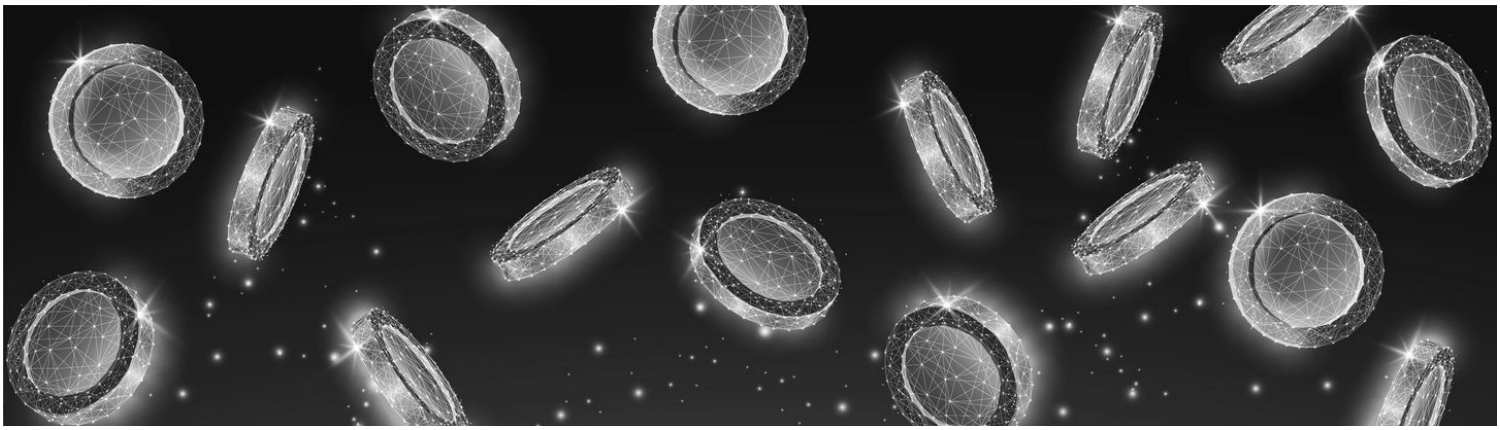
JUNE 2026
APPLIED QUANTUM

THE APPLIED QUANTUM PQC MIGRATION FRAMEWORK

DIGITAL ASSETS EXTENSION



Blockchain, Cryptocurrency, DeFi, and Tokenized Assets *— Industry-Specific Challenges and Framework Adaptations*

Version 2.1 — June 2026

Marin Ivezic
CEO, Applied Quantum
Author, PostQuantum.com

PQCFramework.com | PQCMigrationBrief.com | PostQuantum.com | SecureQuantum.com | AppliedQuantum.com | QuantumReady.com

"Start while it's a project, before it's a crisis."

COPYRIGHT AND LICENSE

DISCLAIMER

This extension is provided as professional guidance based on the author's and Applied Quantum's practitioner experience and publicly available standards, regulations, and industry research. It does not constitute legal, regulatory, financial, compliance, or investment advice. Nothing in this document is a recommendation to hold, sell, migrate, or abandon any digital asset. Organizations should consult qualified legal counsel, auditors, and regulatory authorities for guidance specific to their jurisdiction, sector, and circumstances.

The regulatory timelines, vendor capabilities, algorithm parameters, and tool categories referenced in this document reflect the state of the PQC landscape as of June 2026. These references may become outdated quickly. Readers should verify current status against primary sources before making implementation decisions.

References to specific vendors, products, or tools are for illustrative purposes and do not constitute endorsement. The PQC tooling market is evolving rapidly; products mentioned may have changed in capability, licensing, or availability since publication. Organizations should conduct their own evaluation based on their specific requirements, regulatory environment, and procurement constraints.

NIST IR 8547, referenced throughout for deprecation and disallowance timelines, was an Initial Public Draft as of November 2024 with final publication expected in 2026. Federal agencies and their contractors should reference the final version when available.

ABOUT THIS DOCUMENT

Document type	Enterprise methodology and practitioner framework

Parent Document	The Applied Quantum PQC Migration Framework — Universal — v2.1 (June 2026)
Intended audience	Digital asset custodians, exchange security architects, blockchain protocol developers, DeFi security engineers, institutional crypto investors, and CISOs with digital asset portfolio responsibility
Assumed knowledge	Familiarity with the Universal PQC Migration Framework and its 8-phase lifecycle; working knowledge of blockchain architecture, elliptic curve cryptography (secp256k1, Ed25519, BLS12-381), and digital asset custody
Scope	Digital-asset-specific PQC migration challenges and framework adaptations: blockchain public key exposure, consensus-level migration, smart contract dependencies, proof-of-stake validator security, zero-knowledge proof vulnerabilities, exchange and custodial infrastructure, tokenized assets, and privacy chain retroactive deanonymization. Companion to the Financial Services Extension. Not a standalone document; intended to be used alongside the Universal Framework and the Financial Services Extension.

VERSION HISTORY

Version 1.1 (March 2026): Digital asset content was previously included briefly in the Financial Services Extension v1.1 (March 2026). This v2.0 Digital Assets Extension is the first dedicated publication.

Version 2.0 (June 2026): Initial publication as a dedicated Digital Assets Extension, covering blockchain-specific quantum vulnerabilities informed by Google Quantum AI 2026 resource estimates and the PostQuantum.com ten-article Quantum Threat to Cryptocurrencies deep dive series. Covers 10 digital-asset-specific challenges, phase-by-phase adaptations, regulatory alignment, maturity model supplement, KPI supplement, and recommended immediate actions. Aligned with Universal Framework v2.0.

Version 2.1 (June 2026): Aligned with Universal Framework v2.1. Six new alignment subsections: hybrid and composite signatures (the custodial default versus protocol-governed on-chain schemes); algorithm-specific vulnerability weighting (exposed 256-bit curves as the extreme case); the identity stack in Track B (exchange passkeys, API signing keys, custody console access); SP 800-208 firmware and release signing (hardware wallets, node software, HSMs); securing the CBOM and program artifacts;

verification, decommissioning, and program closure with on-chain specifics. Editorial corrections and companion book cross-reference added.

HOW TO USE THIS EXTENSION

This document is a companion to both the Applied Quantum PQC Migration Framework (Universal) and the Financial Services Extension. It does not replace either document but extends them with digital-asset-specific guidance. The Financial Services Extension covers challenges common to banking, capital markets, insurance, and general financial infrastructure; this Digital Assets Extension goes deeper into blockchain-specific quantum vulnerabilities, consensus-level migration, and the unique governance challenges of decentralized protocols. Readers should have the Universal Framework open alongside this document.

WHAT'S NEW IN V2.1

Version 2.1 of the Digital Assets Extension is a targeted alignment release tracking Universal Framework v2.1 (June 2026):

Alignment with Universal Framework v2.1. Six new alignment subsections map the v2.1 positions that require sector adaptation to digital asset infrastructure: hybrid and composite signatures, and where the custodial default meets protocol-governed on-chain schemes; algorithm-specific vulnerability weighting, with exposed 256-bit curves as the extreme case; the identity stack (exchange passkeys, API signing keys, custody access) within Track B; SP 800-208 stateful hash-based signatures for hardware wallet firmware, node software release signing, and HSM firmware; protection of the CBOM and program artifacts as theft-enabling intelligence; and verification, decommissioning, and program closure with on-chain specifics. The remaining Universal v2.1 additions are sector-neutral and apply as written; the alignment section introduction lists them and the governing cross-references.

Editorial corrections. Minor editorial corrections were applied, and a cross-reference to the companion book, *Quantum Ready*, was added.

WHAT'S NEW IN V2.0

Version 2.0 of the Digital Assets Extension is the first dedicated publication of Applied Quantum's blockchain, cryptocurrency, DeFi, and tokenized-asset PQC migration guidance.

Dedicated digital-asset scope. Digital-asset content has been separated from the Financial Services Extension and expanded into a standalone treatment of blockchain-specific quantum exposure: on-chain public-key exposure, consensus-level migration, smart contract dependencies, proof-of-stake validator security, zero-knowledge proof system vulnerabilities, privacy-chain retroactive deanonymization, exchange and custodial infrastructure, stablecoins, and tokenized real-world assets.

Alignment with Universal Framework v2.0. The parent framework introduced a two-track migration model, deployment-environment classification addressing the FIPS 140-3 validation gap, and updated guidance on public Web PKI. This extension maps those changes to digital-asset infrastructure: custodial APIs and exchange infrastructure in Track A (confidentiality/key exchange); on-chain transaction signatures, validator attestations, smart contract verification, ZK proof systems, and protocol governance in Track B (integrity/signatures/PKI).

New blockchain-specific evidence base. This version incorporates the 2026 Google Quantum AI resource estimates for secp256k1 ECDLP attacks, the on-spend / at-rest / on-setup attack taxonomy, active Bitcoin proposals (BIP-360, BIP-361), Ethereum's pq.ethereum.org post-quantum roadmap, Solana and Algorand PQC experiments, and current digital-asset regulatory signals from MiCA, DORA, and NIST IR 8547.

Scope additions. New coverage includes Bitcoin public-key exposure by script type, Taproot P2TR at-rest regression, unmigrable and dormant coins, Ethereum EOA and admin-key exposure, BLS validator-signature risk, EVM precompile dependencies, KZG and trusted-setup on-setup attacks, Zcash/Monero/Mimblewimble privacy degradation, real-time payment and Layer 2 dependencies, tokenized real-world asset host-chain risk, and digital-asset-specific KPIs and maturity indicators.

ACCOMPANYING RESOURCES

Every aspect of this framework, from executive business cases and cryptographic inventory methodologies to CBOM architecture, hybrid deployment patterns, and vendor governance, has been analyzed in detail on PostQuantum.com over the past 10+ years through practitioner-grounded articles, deep dives, and sector-specific analyses.

The best starting point is the curated Getting Started with Quantum Security and PQC Migration page: https://postquantum.com/starting-pqc-quantum-security/, but readers should also use PostQuantum.com's Search function to surface additional relevant posts that may not be included in that curated list.

Key framework resources, templates, and supporting materials are also published on PQCFramework.com, a dedicated companion site for this framework, drawing on relevant content from PostQuantum.com.

This extension, like the framework it accompanies, is the execution methodology. For the complete treatment (the reasoning behind each phase, extended case examples, and guidance for leading the program from the first board conversation through closure), see the companion book, *Quantum Ready* (QuantumReady.com).

TABLE OF CONTENTS

WHY DIGITAL ASSETS REQUIRES ITS OWN EXTENSION

The Financial Services Extension addresses quantum risks to banking, capital markets, and insurance infrastructure where organizations control their own cryptographic estate and operate under centralized governance. Digital assets present a different kind of migration challenge: cryptographic control is asset control. In traditional finance, compromising a bank's encryption exposes data; in blockchain systems, compromising a private key transfers irreversible ownership of value. For a native permissionless-chain transfer, there is no protocol-level chargeback or universal reversal mechanism. Custodians, stablecoin issuers, and regulated intermediaries may have off-chain legal remedies or contract-level freeze controls, but those are asset- and jurisdiction-specific and do not reverse the base-chain cryptographic failure.

This distinction changes every phase of the PQC migration framework. Discovery means mapping on-chain exposure across script types, not scanning enterprise servers. Risk scoring must account for permanently exposed public keys that cannot be remediated because the private keys are lost. Migration requires consensus-level protocol changes across decentralized networks where no single entity has authority to mandate upgrades. And the threat model includes three distinct attack classes (on-spend, at-rest, and on-setup) that have no direct analogue in enterprise cryptographic migration.

Google Quantum AI's 2026 resource estimates show that breaking the secp256k1 curve protecting Bitcoin and Ethereum requires fewer than 500,000 physical qubits and roughly nine minutes of runtime on a superconducting architecture. Complementary analyses for slower-clock architectures (such as reconfigurable neutral atom qubits) suggest comparable attacks could be feasible with on the order of tens of thousands of physical qubits over multi-day runtimes. Neither machine exists today. Both are smaller than the field assumed twelve months earlier, and the latest Google estimate represents roughly a 20× reduction in physical-qubit requirements for ECDLP-256 compared with prior estimates, continuing a broader pattern of significant resource-estimation improvements.

Cryptography Is the Asset, Not Just the Envelope

In enterprise systems, cryptography protects data and authenticates transactions. The data and the transaction records exist independently of the cryptographic layer; if the cryptography fails, the organization loses confidentiality or integrity, but the underlying assets (money in accounts, records in databases) remain recoverable through legal, regulatory, and institutional mechanisms. In blockchain systems, the cryptographic key is the sole proof of ownership. A quantum attacker who derives a private key from an exposed public key does not merely read data or forge a signature on a message. They take the asset. The transfer is recorded on an immutable ledger with no reversal mechanism. This makes every exposed public key on every major blockchain a potential quantum theft target with a deterministic payout.

Decentralized Governance Without Central Authority

Enterprise PQC migration operates within organizational hierarchies: a CISO can mandate algorithm changes, a board can fund a program, a regulator can set deadlines. Blockchain PQC migration requires consensus among thousands of independent node operators, miners or validators, wallet developers, exchange operators, and users, none of whom answer to a central authority. Bitcoin's BIP process, Ethereum's EIP process, and each alternative chain's governance model impose their own coordination costs, political dynamics, and implementation timelines. When Jameson Lopp proposed BIP-361 to freeze quantum-vulnerable Bitcoin, the community labeled it authoritarian within hours. The engineering for a PQC migration exists; whether decentralized governance can coordinate action against a time-bounded threat is the open question.

Three Attack Classes Without Enterprise Analogue

Google's 2026 whitepaper formalized a taxonomy that organizations managing digital asset exposure should adopt. On-spend attacks target transactions in the mempool before block confirmation (requiring a fast quantum computer). At-rest attacks target public keys already exposed on-chain (requiring only a patient quantum computer with unlimited time). On-setup attacks recover trusted setup parameters from zero-knowledge proof systems, creating permanent classical exploits that require no further quantum access. Enterprise PQC migration does not face this taxonomy because enterprise systems do not publish their public keys on immutable ledgers or rely on trusted setup ceremonies for consensus.

Irreversible Losses and Unmigrable Assets

Approximately 6.7 million BTC (roughly 34% of circulating supply) sits in addresses with exposed public keys, including 1.7 million BTC in Satoshi-era P2PK scripts where the private keys are presumed lost and the funds can never be migrated to quantum-safe addresses. Privacy-preserving blockchains face retroactive deanonymization: a quantum computer could decrypt years of historical shielded Zcash transactions for known addresses, even after the protocol migrates to PQC. No future migration can undo past exposure. These characteristics have no parallel in enterprise PQC migration, where data-at-rest can be re-encrypted and systems can be upgraded.

DIGITAL ASSET-SPECIFIC CHALLENGES

This section details the technical and operational challenges specific to digital asset PQC migration. Each challenge maps to Universal Framework phases and identifies the actors responsible for remediation.

Challenge 1: On-Chain Public Key Exposure

Unlike enterprise systems, where certificate keys and TLS key shares are under operator control and can be rotated or retired, blockchain systems record public-key material on immutable ledgers. The risk is not merely that a public key is visible; it is that the public key is permanently linked to direct asset control with no rotation mechanism. Bitcoin's P2PK scripts store raw public keys; Taproot (P2TR) addresses store tweaked public keys in the locking script; any address that has ever sent a transaction has its public key recorded in the spending input. Ethereum's account model makes an EOA's public key recoverable from the transaction signature once the account sends its first transaction. Legacy EOAs have no native key-rotation mechanism; reducing exposure requires moving assets to a fresh account or adopting account-abstraction mechanisms where available.

This creates an at-rest attack surface measured in trillions of dollars. A quantum attacker with a patient machine (even one requiring hours per key derivation) could methodically work through exposed high-value addresses. The 6.7 million BTC with exposed or reused public-key material represents a material fraction of Bitcoin's circulating supply. Convert to fiat value only with a dated BTC price assumption, as the dollar figure is highly volatile. The exposed Ethereum accounts include addresses controlling smart contract admin keys for stablecoins, bridges, and DeFi protocols managing hundreds of billions in aggregate.

> **Framework Impact:** Phase 1 (Discovery) must include on-chain public key exposure analysis as a primary inventory track. Phase 3 (Risk Scoring) must weight at-rest exposure by value concentration and key recovery feasibility.

Challenge 2: Signature Size and Transaction Throughput

Blockchain transaction throughput is directly constrained by block size or gas limits. PQC signatures are 30 to 60 times larger than the ECDSA signatures they replace. An ML-DSA-44 signature is 2,420 bytes versus 64 bytes for ECDSA P-256 (a 37.8× increase). Bitcoin's 4 MB SegWit block weight limit would accommodate roughly 60% fewer transactions if every signature were replaced with ML-DSA-44. SLH-DSA signatures at security level 1 are 7,856 bytes, which would reduce throughput by over 80%.

FN-DSA (formerly FALCON) offers the most compact PQC signatures at 666 bytes for FN-DSA-512, making it the preferred candidate for blockchain applications. Solana's two core development teams independently selected FALCON-equivalent signatures. However, FN-DSA's implementation complexity (floating-point arithmetic in signing, trapdoor sampling) and its later NIST standardization timeline has slowed adoption. Falcon has been selected by NIST as FN-DSA (FIPS 206), but the final standard remains in development with publication expected around late 2026 or early 2027. The signature size problem directly affects transaction fees, block utilization, state growth, and the economic model of every proof-of-work and proof-of-stake blockchain.

> **Framework Impact:** Phase 5 (Pilots) must include signature-size impact modeling on transaction throughput, fee economics, and state growth. Phase 6 (Infrastructure) must evaluate algorithm selection tradeoffs (ML-DSA security versus FN-DSA compactness) specific to blockchain constraints.

Challenge 3: Consensus-Level Migration Requires Coordinated Hard or Soft Forks

Enterprise PQC migration is an organizational decision. Blockchain PQC migration requires a consensus change that all network participants must adopt. For Bitcoin, this means a soft fork (backward-compatible) or hard fork (backward-incompatible) activated through miner/node signaling. BIP-360 proposes a new output type (P2MR, Pay-to-Merkle-Root) that strips the quantum-vulnerable key path from Taproot, enabling quantum-safe spending without a hard fork. BIP-361 proposes a phased legacy-signature sunset after a post-quantum output type exists. In the current draft, Phase A would stop new deposits to quantum-vulnerable legacy address types after a grace period, while Phase B would restrict ordinary ECDSA/Schnorr spends by requiring a quantum-safe rescue path. Neither has been activated as of June 2026.

Ethereum has a more coordinated protocol-roadmap process around AllCoreDevs, client teams, researchers, and the Ethereum Foundation, which makes migration planning more predictable than Bitcoin's BIP process. Ethereum upgrades still require broad client,

validator, infrastructure, and user adoption. EIP-8141 (Frame Transactions / native account abstraction enabling signature agility) is being considered for the Hegotá hard fork in the second half of 2026. The Ethereum Foundation launched pq.ethereum.org in March 2026 with more than 10 client teams running weekly PQ interoperability devnets. The contrast with Bitcoin's fragmented governance response is significant for migration timeline planning.

For organizations holding digital assets across multiple chains, each chain's governance model and PQC timeline must be tracked independently. There is no cross-chain coordination mechanism for PQC migration.

> **Framework Impact:** Phase 0 (Executive Mandate) must establish monitoring of consensus upgrade proposals across all chains in the organization's portfolio. Phase 4 (Roadmap) must track BIP/EIP/protocol-specific PQC timelines as external dependencies the organization cannot control.

Challenge 4: Unmigrable Assets and Dormant Coins

An estimated 1.7 million BTC in Satoshi-era P2PK scripts have permanently exposed public keys and private keys that are presumed lost. These coins cannot be migrated by normal wallet action if the private keys are lost. If an owner still controls the private key, migration remains possible before a CRQC exists, but the public key is already exposed and the safe-migration window closes once at-rest attacks become realistic. A quantum attacker with sufficient capability could derive the private keys and move the coins. BIP-361's proposal to freeze quantum-vulnerable coins after a grace period generated immediate community backlash, illustrating the governance tension between security and the immutability principle.

This creates a unique risk for the broader ecosystem: if a quantum attacker begins moving long-dormant P2PK coins, even a fraction of the 1.7 million BTC exposure could trigger a market-confidence crisis. Risk models should consider both rapid liquidation and slower quantum-salvage patterns independent of any direct theft from active users. Institutional investors and custodians must model this scenario in their risk frameworks even if their own holdings are properly migrated.

> **Framework Impact:** Phase 3 (Risk Scoring) must include systemic market-impact scenarios from unmigrable asset exposure, not just direct theft risk to the organization's own holdings.

Challenge 5: Smart Contract and DeFi Cryptographic Dependencies

Ethereum's smart contract layer creates compounding quantum risk that has no parallel in Bitcoin or traditional finance. Administrative keys controlling stablecoins (USDT, USDC), cross-chain bridges, lending protocols, and governance contracts represent "low ETH, high leverage" targets where a single compromised key can trigger cascading damage. Hundreds of billions of dollars in stablecoins and tokenized real-world assets sit behind admin keys that are exposed on-chain.

EVM precompiles (ecrecover at address 0x01, ecAdd/ecMul/ecPairing at 0x06–0x08) hardcode secp256k1 and BN254 curve operations into the execution environment. Smart contracts that verify signatures on-chain using these precompiles cannot be made quantum-safe without new PQC precompiles at the consensus level, a dependency that individual contract deployers cannot resolve. Contracts locked behind timelocks, multisig arrangements, or immutable proxy patterns may be permanently unable to upgrade their cryptographic dependencies.

> **Framework Impact:** Phase 1 (Discovery) must include smart contract admin key exposure mapping across all chains and protocols in the organization's portfolio. Phase 7 (Vendor Governance) must include DeFi protocol developers and smart contract audit firms in PQC readiness assessment.

Challenge 6: Proof-of-Stake Consensus Vulnerability

Ethereum's Proof-of-Stake consensus uses BLS signatures on the BLS12-381 curve for validator attestations and block proposals. Approximately 36 million ETH is staked across roughly 1.1 million validators. A quantum attacker targeting validator keys could halt finality (by compromising more than one-third of stake), control fork choice (more than one-half), or finalize inconsistent chains (more than two-thirds). Unlike Bitcoin's Proof-of-Work (which is not Shor-vulnerable in the way elliptic-curve signatures are. Quantum search could affect hash-based mining economics through at most quadratic speedups, but it does not create the same direct key-recovery failure mode as Shor's algorithm against ECDSA or BLS signatures), PoS consensus security depends entirely on the hardness of the elliptic curve discrete logarithm problem.

Other PoS chains (Solana, Cardano, Polkadot, Cosmos, Avalanche) face similar validator-key exposure, each on their own curve and signature scheme. The migration path requires replacing validator signature schemes at the consensus level, which in turn requires coordinated hard forks across each chain.

> **Framework Impact:** Phase 3 (Risk Scoring) must include PoS consensus integrity as a systemic risk category separate from individual key compromise. Phase 4 (Roadmap) must track PoS chains' PQC consensus upgrade timelines.

Challenge 7: On-Setup Attacks and Zero-Knowledge Proof Systems

Certain blockchain protocols rely on trusted setup ceremonies that generate secret parameters. If a quantum computer recovers those parameters, it creates a permanent, reusable classical exploit requiring no further quantum access. Ethereum's KZG polynomial commitments (used for Data Availability Sampling) on BLS12-381 are vulnerable: recovering the "toxic waste" from the public parameters would allow an attacker to forge data availability proofs indefinitely using a conventional computer. Zcash's Sapling shielded pool (which uses Groth16 over BLS12-381 with a trusted setup), and any ZK proof system built on pairing-based curves with a trusted setup (such as KZG) share the same on-setup vulnerability class. Note: Mimblewimble Pedersen commitments use transparent generators (not a trusted setup), so while they are quantum-vulnerable to standard discrete-log attacks, they do not carry the on-setup "toxic waste" risk.

On-setup attacks differ from on-spend and at-rest attacks in a critical way: a single quantum computation creates an exploit that can be stockpiled, sold, or deployed at scale without any further quantum capability. The affected protocols must be replaced entirely; patching the cryptographic layer is insufficient because the compromise is in the public parameters themselves.

> **Framework Impact:** Phase 3 (Risk Scoring) must classify on-setup vulnerabilities at the highest severity because they create permanent classical exploits. Phase 5 (Pilots) must prioritize protocols with trusted setup dependencies for early migration.

Challenge 8: Privacy Chain Retroactive Deanonymization

Privacy-preserving blockchains (Zcash shielded pools, Monero ring signatures, Mimblewimble, Tornado Cash, Aztec) face a quantum threat that no future migration can fully address: retroactive deanonymization of historical transactions. Encrypted transaction data recorded on-chain today will become readable to a future quantum computer. For Zcash, this means years of shielded transaction graphs could be reconstructed for addresses with known public keys. For Monero, ring signature anonymity sets could be reduced or eliminated. Even after these protocols migrate to PQC, the historical data remains on-chain and vulnerable.

This is the digital asset equivalent of Harvest Now, Decrypt Later (HNDL), but with a critical difference: in enterprise systems, re-encryption of stored data is possible. On an immutable blockchain, historical ciphertext cannot be replaced. The privacy guarantees that users relied on when transacting become retroactively void.

> **Framework Impact:** Phase 3 (Risk Scoring) must account for retroactive privacy loss as an irreversible risk that cannot be mitigated by future migration. Organizations with regulatory exposure to historical privacy-chain transactions should assess this risk now.

Challenge 9: Exchange and Custodial Infrastructure

Centralized exchanges and custodial platforms manage the intersection of enterprise infrastructure and blockchain-specific quantum risk. Their internal systems (HSMs, key management, API authentication, TLS) face the same PQC challenges as any financial institution. Their on-chain operations (hot wallets, cold storage, withdrawal processing) face blockchain-specific exposure. Exchanges managing millions of customer accounts must assess address reuse across their entire UTXO management strategy, evaluate public key exposure for every custodial address, and plan for PQC signature support across every chain they list.

Coinbase's Quantum Advisory Council published a 2026 position paper on quantum computing and blockchain, emphasizing that crypto is safe today but that ecosystem-wide migration will take years and should begin before the threat becomes urgent. The paper recommended prioritizing HSM and KMS upgrades, implementing crypto-agility in signing infrastructure, and establishing quantum readiness metrics. While valuable as an industry signal, the Coinbase approach focuses primarily on custodial infrastructure and does not address the on-chain exposure of customer funds in UTXO-based systems or the smart contract dependencies in DeFi.

> **Framework Impact:** Phase 1 (Discovery) must cover both enterprise infrastructure (HSMs, APIs, TLS) and on-chain exposure (address reuse, public key exposure, chain-specific vulnerabilities). Phase 7 (Vendor Governance) must include blockchain node software providers and wallet SDKs.

Challenge 10: Tokenized Real-World Assets and Stablecoins

The tokenized asset market (projected by Citi to reach approximately $5.5 trillion by 2030 in its base case, with upside scenarios extending into the high single-digit trillions depending on adoption) inherits the quantum vulnerabilities of its host chains. Tokenized treasuries, real estate, commodities, and private credit instruments sit in smart contracts

secured by the same quantum-vulnerable elliptic curve cryptography as native chain assets. Stablecoins (USDT, USDC, DAI, and others) now represent over $300 billion in aggregate market capitalization, controlled through various admin key structures (minter, pauser, blacklist, upgrade, bridge roles) on Ethereum and other chains.

For institutional investors and regulated entities, the quantum risk to tokenized assets is a fiduciary and regulatory concern. If the host chain's cryptography is compromised, the tokenized representation of a real-world asset becomes unrecoverable through on-chain mechanisms, even though the underlying asset (a treasury bond, a property deed) continues to exist off-chain. The legal and operational frameworks for recovering tokenized assets after a quantum-driven chain compromise do not exist. Organizations issuing or holding tokenized assets should assess their host chain's PQC roadmap as a material risk factor.

> **Framework Impact:** Phase 0 (Business Case) should include tokenized asset quantum exposure as a fiduciary risk. Phase 3 (Risk Scoring) must evaluate host chain PQC readiness for every tokenized asset in the portfolio.

ALIGNMENT WITH UNIVERSAL FRAMEWORK V2.1

The Universal Framework v2.0 changes have specific implications for digital asset infrastructure, and v2.1 added positions and sections that digital asset organizations need to map onto their programs. This section covers both: the three v2.0 foundations below, followed by the v2.1 positions that require digital-asset-specific adaptation. The remaining Universal v2.1 additions (the data-at-rest decision framework in Activity 5.6, the AI-assisted migration position in 5.7 with its Phase 1 tool category, cloud and SaaS shared responsibility in 7.7, the Accelerated Execution Profile in 4.7, the risk-weighted coverage KPI, algorithm sovereignty and standards fragmentation, crisis communications, the skills matrix, and Appendices G and H) apply as written, with two notes. The data-at-rest framework governs off-chain stores (custody records, key shards and backups, KYC archives); on-chain data is public by design, and its exposure is covered by the algorithm-weighting analysis in this section. And the Universal's counterparty coordination pattern (Activity 7.6) reaches its extreme case in protocol-governed migration, where the counterparty is a governance process no single participant can compel; this extension's protocol-migration guidance is that case.

Two-Track Migration Model in Digital Assets

Track A (Confidentiality / Key Exchange): Exchange API TLS endpoints, custodial platform communications, inter-exchange settlement channels, wallet-to-node RPC connections, and VPN tunnels protecting node infrastructure. This track is largely within custodial operators' control and can begin immediately using hybrid ML-KEM key exchange.

Track B (Integrity / Signatures / PKI): On-chain transaction signatures (secp256k1, Ed25519, BLS12-381), smart contract verification (EVM precompiles, Solana BPF programs), validator attestations (BLS in PoS), zero-knowledge proof systems (KZG, Groth16), and code-signing for node software releases. This track requires consensus-level protocol changes that individual organizations cannot implement unilaterally.

The critical difference from enterprise migration: Track B in digital assets depends on decentralized governance decisions across each blockchain protocol. Organizations can execute Track A independently; Track B requires monitoring and participating in protocol governance processes.

FIPS Validation Gap in Digital Assets

Regulated custodial platforms and exchanges operating in jurisdictions requiring FIPS-validated cryptography face the same validation gap as other financial institutions. The absence of FIPS 140-3 validated PQC modules constrains production HSM deployment for custodial key management. Unregulated or DeFi-native operations typically do not face FIPS requirements, creating a bifurcated migration landscape where regulated and unregulated entities face different constraint profiles.

Ecosystem PQC Readiness Varies Widely

The blockchain ecosystem's quantum readiness ranges from leading-edge to nonexistent. The Quantum Resistant Ledger (QRL) has been post-quantum since inception in 2018. Algorand executed its first PQC-secured transaction in 2025. Solana's two core teams independently selected FALCON-equivalent signatures. Zcash targets full post-quantum security by 2027. The Ethereum Foundation launched pq.ethereum.org in March 2026 with weekly PQ interoperability devnets. Bitcoin has no activated PQC proposal as of June 2026. Organizations must assess PQC readiness chain by chain, not assume ecosystem-wide progress.

Hybrid and Composite Signatures: Where the Default Applies

Universal v2.1 takes the position that composite or dual signatures (classical plus PQC) are the default for Track B wherever toolchains support them, with solo ML-DSA treated as a recorded risk decision. In digital assets that default splits along the control boundary. For infrastructure the organization controls (custodial signing systems, node software release signing, attestation services, API request signing) the composite default applies as written, and HSM-backed or threshold signing infrastructure can carry dual signatures today. For on-chain signature schemes, the choice is protocol-governed and block-space-constrained: a composite signature is larger still than the ML-DSA that already cuts Bitcoin throughput by roughly 60%, which is precisely why compactness drives blockchain algorithm selection (FN-DSA) and why composite schemes are unlikely on-chain. Organizations cannot record a risk decision for a protocol they do not control, but they should document the gap (which holdings sit on chains with solo-PQC or no-PQC

trajectories) as an accepted ecosystem risk in Phase 3. Where account abstraction provides signature agility (EIP-8141-style validation logic), adding PQC verification alongside classical is the closest on-chain analogue to the hybrid default and worth piloting as it matures.

Algorithm Weighting: The Extreme Case

Universal v2.1 introduces algorithm-specific vulnerability weighting in Phase 3: quantum attack cost scales with key size, not classical strength, so 256-bit elliptic curves sit at the front of the attack queue. Digital assets are the extreme case of this weighting, for two compounding reasons. First, the entire asset class runs on 256-bit curves (secp256k1, Ed25519, BLS12-381) with no RSA legacy to dilute the exposure. Second, for every exposed public key on-chain (Challenge 1), the harvest step is already complete: the attacker needs no interception, no breach, and no waiting, because the key material and the value it controls are published on an immutable public ledger. For institutions running Phase 3 scoring across a combined traditional and digital asset estate, exposed on-chain value and custody signing keys therefore rank above RSA-2048 enterprise systems and above unexposed ECC estates. Record curve, exposure status (exposed versus hash-protected), and value at risk for every digital asset CBOM entry so the weighting applies mechanically.

The Identity Stack in Track B

Universal v2.1 brings the identity stack explicitly into Track B scope, and in digital assets the identity layer guards the signing infrastructure itself. Exchange and custodial customer authentication is moving onto passkeys (FIDO credentials on P-256, already standard at major exchanges), trading and custody APIs authenticate with long-lived API keys and request-signing keys, withdrawal approval workflows rely on device-bound credentials, and workforce access to custody consoles and key ceremonies runs on enterprise identity (OIDC, SAML, hardware tokens). A quantum adversary who can forge the identity layer does not need to break the vault. Carve an identity slice in the Phase 1 inventory: identity providers, token and request signing keys, authenticator inventory, federation chains into custody platforms, and put the credential migration question (how enrolled passkeys and device-bound credentials will be re-enrolled when signature algorithms change) into Phase 7 governance for authentication and custody platform vendors. Short-lived session tokens are low priority; the signing keys and enrolled credentials behind them are standard Track B targets.

SP 800-208: Firmware and Release Signing

Universal v2.1 foregrounds stateful hash-based signatures (LMS and XMSS, NIST SP 800-208) as the component of Track B that deploys now, and digital assets has three natural targets. Hardware wallet firmware is the sharpest: the firmware verification key baked into a device at manufacture must remain trustworthy for the many years that device spends in a drawer securing assets, so verification keys provisioned today must outlive the arrival of a CRQC. Node software release signing (Bitcoin Core, Ethereum clients, validator software) and custody HSM firmware follow the same logic. LMS and XMSS are standardized, conservative, and required by CNSA 2.0 for exactly this use; the state-management constraint that makes them unsuitable for general-purpose signing is satisfied by the controlled release ceremonies that wallet vendors, client teams, and custody operators already run. The action: move firmware and release signing pipelines to SP 800-208 signatures now, dual-signed with classical during transition, and add hardware wallet PQC verification capability to the Phase 7 vendor questions for wallet providers.

Securing the CBOM and Program Artifacts

Universal v2.1 adds Activity 2.5: the CBOM and migration program artifacts are themselves high-value targets. Nowhere is the stake higher than in digital assets, where key compromise is immediate, irreversible theft. A digital asset CBOM maps cold storage architecture, signing infrastructure topology, address-to-value relationships, admin key custody arrangements, and the list of not-yet-migrated exposure: collectively, a heist plan. External parties have legitimate claims on parts of this material: SOC 2 auditors, proof-of-reserves attestation providers, and regulators under MiCA and DORA. Apply Activity 2.5's controls without exception: external parties receive point-in-time extracts scoped to their engagement, never standing access to the queryable inventory; the CBOM repository is monitored with the same severity as the key management systems it describes; and access to it appears on the SOC's high-sensitivity exfiltration watch list.

Verification, Decommissioning, and Closure On-Chain

Universal v2.1 adds a Migration Verification & Program Closure section, and digital assets gives it a twist in both directions. Verification is partly public: on-chain migration is independently observable, since anyone can confirm that funds moved to quantum-resistant address types: unusually strong evidence, with the corollary that incomplete migration is equally visible to attackers. Custodial-side verification follows the Universal standard: observed algorithm negotiation on API and platform connections, and negative testing once policy requires refusing classical-only peers. Decommissioning carries the

harder twist: an exposed public key cannot be decommissioned, because chain history is immutable. The only decommissioning available is moving value off the exposed key, then destroying the corresponding HSM-held material with certificates per the Universal evidence standard; the on-chain record remains, permanently, as a reminder that in this sector exposure is forever. Closure must also account for dependencies that outlast the program: protocol-level PQC timelines (BIP-360/361 activation, client PQC rollouts) will run for years after custodial migration completes, so closure criteria should hand protocol monitoring and governance participation to a standing function rather than declaring the external dependency resolved.

PHASE-BY-PHASE FRAMEWORK ADAPTATIONS FOR DIGITAL ASSETS

Phase 0 — Executive Mandate & Business Case

1. **Fiduciary risk framing:** Frame the quantum threat as a fiduciary and custody risk, not just a technology risk. Institutional holders of Bitcoin, Ethereum, and tokenized assets have a duty to assess whether the cryptographic foundations of their holdings are quantum-vulnerable and to document their assessment and response plan.

2. **Market-impact scenario modeling:** Model the systemic impact of quantum-derived key theft on market prices, exchange liquidity, and custody insurance. The sudden appearance of 1.7 million unmigrable BTC on exchanges would constitute a market event independent of any direct loss to the organization.

3. **Governance participation:** Allocate resources for participating in BIP, EIP, and protocol-specific governance processes. PQC migration on public blockchains requires community coordination that the organization should influence, not merely observe.

Phase 1 — Discovery & Inventory

Digital Asset-Specific Inventory Tracks

1. **On-chain public key exposure:** For every chain in the portfolio, analyze UTXO/account exposure: how many addresses have exposed public keys (spent from, P2PK, P2TR, Ethereum EOAs), what value is at risk, and whether migration to hash-protected or quantum-safe addresses is possible.

2. **Smart contract cryptographic dependencies:** Map all smart contracts the organization interacts with (DeFi protocols, stablecoins, bridges, oracles) and identify their admin key exposure, precompile dependencies, and upgrade mechanisms.

3. **Custodial infrastructure:** Inventory HSMs, key management systems, signing infrastructure, API authentication, and TLS configurations across all custodial platforms and exchange integrations.

4. **Validator/staking infrastructure:** For PoS chains, inventory validator key management, BLS signature implementations, and slashing protection mechanisms.

5. **Layer 2 and bridge dependencies:** Map Lightning Network channel exposure, cross-chain bridge cryptographic dependencies, rollup proof systems, and state channel implementations.

Phase 2 — CBOM & Documentation

Build the digital asset CBOM in layers: (1) custodial infrastructure cryptography the organization controls directly, (2) on-chain cryptographic dependencies determined by protocol rules the organization cannot change, and (3) smart contract cryptographic dependencies managed by third-party protocol developers. Document the governance mechanism and timeline for each layer's PQC transition.

Phase 3 — Risk Scoring & Prioritization

Digital Asset Priority Tiers

Priority	System Category	Rationale
Tier 1	Custodial HSM/KMS infrastructure, hot wallet signing systems, exchange API authentication	Directly controlled by the organization. Highest operational impact if compromised. Can begin migration independently.
Tier 2	On-chain exposure: high-value UTXO addresses with exposed public keys, smart contract admin keys, validator keys	High value at risk. Migration depends on protocol-level PQC support (BIP-360, EIP-8141) or address hygiene improvements.
Tier 3	Smart contract dependencies: DeFi protocol interactions, stablecoin admin keys, bridge collateral, oracle feeds	Value at risk but remediation depends on third-party protocol developers. Monitor and engage through governance.

Tier 4	Layer 2 infrastructure (Lightning, rollups), privacy chain exposure, ZK proof system dependencies, tokenized asset host-chain risk	Complex dependencies. Migration requires coordinated protocol upgrades across multiple layers.

Phase 4 — Roadmap & Governance

Protocol-Specific Timeline Map

1. **Bitcoin:** BIP-360 (P2MR quantum-safe output type) and BIP-361 (legacy signature sunset) proposals. No activation timeline as of June 2026. Monitor Bitcoin Core development and miner signaling.
2. **Ethereum:** EIP-8141 (signature agility via account abstraction) targeting Hegotá hard fork (second half 2026). pq.ethereum.org weekly PQ devnets. Core PQ infrastructure completion targeted approximately 2029.
3. **Solana:** Two core teams (Anza/Agave and Firedancer/Frankendancer) independently selected FALCON-equivalent signatures. Monitor SIMD proposals for PQC integration timeline.
4. **Zcash:** Targets full post-quantum security by 2027, including the deprecation of legacy Sapling pools (Zcash already moved to Orchard/Halo 2 in 2022, eliminating the trusted-setup dependency) and a transition to entirely PQC-native shielded proofs.
5. **NIST IR 8547:** Proposes deprecating ECDSA by 2030 and disallowing by 2035. Sets the outer boundary for any chain that has not migrated.

Phase 5 — Pilots & Migration

1. **Custodial infrastructure hybrid TLS:** Enable hybrid ML-KEM + X25519 on exchange APIs and custodial platform endpoints. Lowest-risk starting point.
2. **Address hygiene enforcement:** Eliminate address reuse across all custodial UTXO management. Move funds from Taproot (P2TR) addresses to hash-protected SegWit addresses to reduce at-rest exposure.

3. **PQC signature testing on testnets:** Deploy PQC transaction signing on Bitcoin Signet, Ethereum Sepolia for application tests and Hoodi (or current equivalent) for validator tests, and Solana devnet to measure signature size impact on throughput, fees, and client compatibility.

4. **Validator key PQC migration:** For PoS chains with PQC validator support, pilot validator key migration in testnet environments before mainnet deployment.

Phase 6 — Infrastructure & Performance

1. **HSM PQC readiness for custodial signing:** Assess whether custodial HSMs support PQC key generation and signing within the FIPS-validated boundary. Plan firmware upgrades or hardware replacement.

2. **Transaction throughput impact modeling:** Benchmark PQC signature sizes against block size/gas limits for each chain. Model fee impact, state growth, and mempool behavior with PQC-sized transactions.

3. **Node software compatibility:** Track PQC support across node implementations (Bitcoin Core, Geth/Nethermind/Besu, Solana validator clients) and wallet SDKs.

Phase 7 — Vendor & Supply Chain Governance

Vendor Category	Examples	Engagement Approach
Protocol development teams	Bitcoin Core, Ethereum Foundation, Solana Labs/Anza, Zcash Foundation	Monitor BIP/EIP/SIMD proposals. Participate in governance. Fund PQC development where appropriate.
Custodial/exchange platforms	Coinbase, Binance, Kraken, BitGo, Fireblocks, Anchorage	PQC readiness questionnaires. HSM upgrade timelines. Address reuse audit.
Wallet software providers	Ledger, Trezor, MetaMask, Phantom, Electrum	Monitor PQC signature support. Hardware wallet PQC capability timelines.
Smart contract audit firms	Trail of Bits, OpenZeppelin, Certora, Consensys Diligence	Include quantum vulnerability assessment in smart contract

		audits. Admin key exposure analysis.
HSM and key management vendors	Thales, Utimaco, Futurex, Entrust, AWS KMS, Azure Key Vault, GCP Cloud KMS	Same engagement as Financial Services Extension. PQC firmware and validation timelines.

DIGITAL ASSETS REGULATORY ALIGNMENT MAP

Digital asset regulation is fragmented across jurisdictions, but several regulatory developments intersect with PQC migration planning.

Regulatory Body / Standard	Key Requirement	Timeline	Framework Phase(s)
NIST IR 8547	Deprecate ECDSA/RSA at 112-bit after 2030; disallow after 2035	2030/2035	Phase 3, Phase 4
EU MiCA	Crypto-asset service providers must maintain robust ICT security	Effective December 2024	Phase 0, Phase 1
EU DORA	State-of-the-art cryptography and crypto-agility requirements for financial entities including crypto-asset service providers	Effective January 2025	Phase 0 through Phase 5
SEC / OCC / CFTC (US)	Evolving custody and security requirements for digital asset custodians	Ongoing	Phase 0, Phase 7
HKMA / MAS / JFSA (Asia)	Quantum readiness expectations for regulated virtual asset service providers	Various 2026-2027	Phase 0, Phase 4

BIS / FSB	Financial stability implications of quantum-vulnerable digital assets; tokenized asset risk frameworks	Ongoing	Phase 0, Phase 3

The regulatory gap is significant: no jurisdiction has explicitly mandated PQC migration for blockchain-native assets. However, regulated custodians, exchanges, and tokenized asset issuers now fall under broader financial regulation (MiCA, DORA, SEC custody rules) that will incorporate PQC expectations as they evolve. Organizations should prepare for this convergence.

DIGITAL ASSETS MATURITY MODEL SUPPLEMENT

Level	Universal Indicator	Digital Asset Indicator
1 — Aware	Quantum risk acknowledged; no formal program	No assessment of on-chain public key exposure. No inventory of custodial HSM PQC readiness. No monitoring of protocol-level PQC proposals (BIPs, EIPs).
2 — Assessed	Cryptographic inventory underway; initial risk assessment completed	On-chain exposure quantified by chain and address type. Custodial HSM estate mapped. Smart contract admin key exposure assessed. Protocol PQC timelines tracked. Initial QRA produced.
3 — Planning	Roadmap established; pilots designed; governance operational	Protocol-specific PQC timeline map maintained. Address hygiene enforced (no reuse, no unnecessary Taproot exposure). Custodial hybrid TLS pilots designed. Industry governance participation active.
4 — Migrating	Pilots in production; wave-based migration underway	Hybrid PQC on custodial APIs. PQC signing tested on testnets. Funds migrated from exposed addresses where possible. Validator keys on PQC-ready infrastructure.
5 — Resilient	Crypto-agility achieved; algorithm transitions routine	All custodial infrastructure quantum-safe. On-chain holdings on PQC-native address types. Smart contract interactions limited to PQC-upgraded protocols. Algorithm rotation capability across chains.

DIGITAL ASSETS KPI SUPPLEMENT

Board-Level KPIs (Quarterly)

1. **On-chain quantum exposure:** Value held in addresses with exposed public keys / total custodial value. Target: converging toward zero through address migration.
2. **Custodial infrastructure PQC readiness:** Percentage of custodial HSMs and signing systems with PQC capability / total custodial infrastructure.
3. **Protocol PQC timeline alignment:** Number of chains in portfolio with activated PQC support / total chains held. Tracking metric for external dependency.
4. **Smart contract admin key exposure:** Value controlled by smart contracts with quantum-vulnerable admin keys / total smart contract exposure.

Operational KPIs (Monthly)

1. **Address reuse rate:** Number of custodial addresses reused for spending / total custodial addresses. Target: zero.
2. **Protocol governance engagement:** BIP/EIP/SIMD PQC proposals tracked and assessed / total active PQC proposals across portfolio chains.
3. **Custodial API PQC coverage:** Exchange and custodial API endpoints with hybrid PQC enabled / total endpoints.

RECOMMENDED IMMEDIATE ACTIONS

For organizations holding or managing digital assets at Maturity Level 1 (Aware) or Level 2 (Assessed), these actions can begin immediately.

#	Action	Timeline	Phase
1	Quantify on-chain public key exposure across all chains: UTXO address types, Ethereum EOA exposure, validator key exposure, smart contract admin keys.	0–3 months	Phase 1
2	Eliminate address reuse in all custodial UTXO management. Move funds from Taproot (P2TR) addresses to new, never-before-spent-from hash-protected SegWit (P2WPKH) addresses. This reduces at-rest exposure only and does not make Bitcoin quantum-safe against future on-spend attacks.	0–3 months	Phase 5
3	Map custodial HSM/KMS estate by model, firmware, and PQC readiness. Initiate vendor engagement on PQC signing capability.	0–3 months	Phase 1/7
4	Enable hybrid PQC (ML-KEM-768 + X25519) on at least one exchange or custodial API endpoint.	3–9 months	Phase 5
5	Establish protocol governance monitoring for BIP-360/361, EIP-8141, Solana SIMDs, and Zcash PQC proposals.	0–3 months	Phase 0/4
6	Assess smart contract admin key exposure for all DeFi protocols and stablecoins in the portfolio. Document remediation paths (key rotation, multisig upgrades, protocol migration).	0–6 months	Phase 1/3
7	Deploy PQC transaction-signing experiments on appropriate test environments (Bitcoin regtest,	3–9 months	Phase 5

	custom Signet, or BIP-360-enabled test forks; Ethereum Sepolia) to measure signature size, throughput impact, and wallet compatibility.		
8	Model market-impact scenarios from unmigrable BTC exposure and systemic PoS validator compromise.	0–6 months	Phase 3

FURTHER READING

The following PostQuantum.com articles provide detailed analysis supporting this extension:

1. **Deep Dive: The Quantum Threat to Cryptocurrencies — https://postquantum.com/quantum-threat-cryptocurrencies/ —** Ten-article series covering resource estimates, platform vulnerabilities, migration roadmaps, and governance.

2. **Bitcoin's Quantum Vulnerability: Anatomy of the Attack Surface — https://postquantum.com/quantum-threat-crypto/bitcoin-quantum-vulnerability/ —** Script-type taxonomy, 6.7M BTC exposure analysis, Taproot regression.

3. **Ethereum's Five Quantum Vulnerabilities — https://postquantum.com/quantum-threat-crypto/ethereum-quantum-vulnerabilities/ —** Account signatures, admin keys, EVM precompiles, PoS consensus, KZG commitments.

4. **Fixing Bitcoin: The Post-Quantum Migration Technical Roadmap — https://postquantum.com/quantum-threat-crypto/fixing-bitcoin-pqc-migration/ —** BIP-360, algorithm tradeoffs, UTXO migration mechanics, emergency escape hatches.

5. **Preparing for Crypto's Quantum Future: A Practical Guide — https://postquantum.com/quantum-threat-crypto/preparing-crypto-quantum-future/ —** Actions segmented by role: holders, exchanges, developers, investors, regulators.

6. **Coinbase Quantum Blockchain Paper Analysis — https://postquantum.com/security-pqc/coinbase-quantum-blockchain-paper-analysis/ —** Critical assessment of Coinbase's four-phase quantum resilience framework.

7. **Google Quantum AI's ECDLP Resource Estimates — https://postquantum.com/security-pqc/google-quantum-bitcoin-ecdlp/ —** Analysis of the 2026 paper showing <500K qubit requirement for secp256k1.

8. **Hybrid Cryptography for the Post-Quantum Era — https://postquantum.com/post-quantum/hybrid-cryptography-pqc/ —** Hybrid schemes in TLS, SSH, IPsec; standards alignment; pilot design.

9. **Rethinking CBOM — https://postquantum.com/post-quantum/rethinking-cbom/ —** Minimum Viable CBOM approach applicable to digital asset infrastructure.

ABOUT

ABOUT THE AUTHOR

Marin Ivezic is a former Fortune Global 500 CISO/CTO, the Editor-in-Chief of PostQuantum.com, and the founder and CEO of Applied Quantum. He previously held cybersecurity partner and practice lead roles, including regional and global leadership positions, at IBM, Accenture, PwC, and KPMG. He is also the former CEO of Cyber Agency and the founder of Cryptosec, a cryptography advisory and engineering firm.

Marin has been involved in quantum technologies for over 25 years, having advised governments on the quantum threat since the early 2000s. He previously founded Boston Photonics and PQ Defense. He has led real-world quantum readiness programs for telecoms, financial institutions, and critical infrastructure operators, including programs exceeding 120,000 discrete migration tasks.

PostQuantum.com, his personal blog, reaches over 1 million monthly readers and is recognized as the premier quantum security publication for CISOs, CTOs, and security architects worldwide.

QUANTUM READY: THE COMPANION BOOK

Quantum Ready (QuantumReady.com) is the book-length companion to this framework, written by the same author. Where this document is deliberately methodology-grade (prerequisites, activities, outputs, decision logic). The book provides the complete treatment: the reasoning behind each phase, extended case examples from real migration programs, sector narratives, and guidance for leading the program from the first board conversation through closure. The two are maintained in alignment: the framework is updated as the field moves, and the book supplies the depth that a methodology document omits by design.

ABOUT APPLIED QUANTUM

Applied Quantum (AppliedQuantum.com) is a research-driven professional services firm focused entirely on quantum technologies and post-quantum security. Its dedicated security practice, Secure Quantum (SecureQuantum.com), focuses on quantum security advisory and PQC migration. Services span Quantum Security & PQC Migration, Quantum Strategy & Sovereignty, Quantum Engineering & Implementation, and Quantum Commercialization.

If you need help: Applied Quantum provides advisory, program design, and hands-on migration execution support. Contact: contact@appliedquantum.com