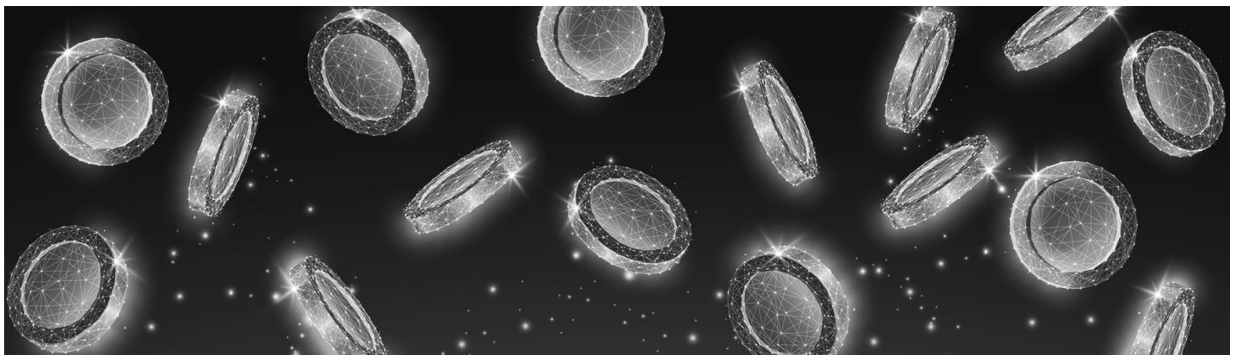
SEPTEMBER 2026

APPLIED QUANTUM

THE APPLIED QUANTUM PQC MIGRATION FRAMEWORK

DIGITAL ASSETS EXTENSION



Custody, exchanges and distributed ledgers *– sector-specific challenges and framework adaptations*

Version 3.0 – September 2026

Marin Ivezic

CEO, Applied Quantum

Author, PostQuantum.com

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

COPYRIGHT AND LICENSE

DISCLAIMER

This framework 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, or compliance advice. 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 PQC as of September 2026. These references may become outdated quickly. Readers should verify current status against primary sources before making implementation decisions; movement between editions is published through the PQC Migration Brief.

References to specific vendors, products, or tools are for illustrative purposes and do not constitute endorsement.

NIST IR 8547, referenced throughout for deprecation and disallowance timelines, remains an Initial Public Draft at the date of this edition; the deprecation and disallowance dates it proposes are cited as anchors and re-checked at each release. Federal agencies and their contractors should reference the final version when it publishes.

ABOUT THIS DOCUMENT

Document type	Enterprise methodology and practitioner framework
Parent document	The Applied Quantum PQC Migration Framework – Universal – v3.0 (September 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 v3.0 and its 8-phase lifecycle; working knowledge of blockchain architecture, elliptic curve cryptography (secp256k1, Ed25519, BLS12-381), digital asset custody and protocol governance
Scope	Digital-asset-specific PQC migration challenges and framework adaptations: on-chain public key exposure by state, consensus-level

	migration and the protocol as a counterparty, smart contract dependencies, proof-of-stake validator security, zero-knowledge proof vulnerabilities including the shared-verifier-defect failure mode, exchange and custodial infrastructure as the migratable surface, tokenized assets, and privacy chain retroactive deanonymization. Companion to the Financial Services Extension (v3.0, September 2026). Not a standalone document; intended to be used alongside the Universal Framework and the Financial Services Extension.
Status	Version 3.0 - published September 2026

VERSION HISTORY

Version	Date	Changes
2.0	June 2026	Major version. Three methodological changes: (1) two-track migration model separating key exchange (HNDL) and signature/PKI (TNFL) as parallel tracks; (2) PKI architecture fork with definitive position on Merkle Tree Certificates for public Web PKI; (3) FIPS 140-3 validation gap as hard deployment constraint with environment classification. New Program Foundation sections: SOC Implementation (five detection use cases, four incident response playbooks, five tabletop exercises, three-horizon quantum CTI model), GRC Implementation (17-indicator cascading KRI framework, risk appetite statements, regulatory intelligence process, audit and assurance, GRC-SOC handoff). Expanded Program Foundations: Governance (program leadership, board oversight, three lines of defense), Crypto-Agility (five-dimensional operational discipline with four-year implementation roadmap), Skills & Team Structure (team sizing, build/borrow/buy framework, crypto champion program). Also added: cost estimation methodology, NIST CSWP 39 crypto-agility alignment, 2026–2030 regulatory deadline convergence analysis, multinational hybrid navigation framework, deployment ecosystem status data, algorithm pipeline update (9 additional signature candidates, FN-DSA/HQC status, CNSA 2.0 requirements), objection-handling appendix (Appendix F). All sector extensions updated to v2.0.
2.1	June 2026	Targeted update. Activity 3.3 sequencing harmonized with the two-track model; explicit position on hybrid/composite signatures; algorithm-specific vulnerability weighting added to Phase 3 risk scoring (ECC/RSA quantum resource analysis); SP 800-208 hash-based signatures foregrounded as the deploy-

Version	Date	Changes
		now component of Track B. New: Activity 2.5 (Secure the CBOM and Program Artifacts), Migration Verification & Program Closure section, identity and authentication stack in Track B scope. Added: reference program economics (0.2c), confidentiality-horizon method (1.1), evidence dossier as litigation defense, M&A due diligence, procurement model-language references, additional common failures and benefit arguments. Web PQC adoption datapoint corrected to F5 Labs mid-2025 attribution. Companion book (Quantum Ready) cross-references added. Also added: data-at-rest decision framework (5.6); AI-assisted migration position (5.7) with a Phase 1 tool category; counterparty coordination (7.6); cloud shared responsibility and SaaS (7.7); Accelerated Execution Profile (4.7); risk-weighted coverage KPI; algorithm sovereignty and standards fragmentation; crisis communications and industry information sharing (GRC); skills matrix; role-based reading paths and right-sizing profiles; Appendix G (framework crosswalk); Appendix H (protocol coverage matrix).
3.0	September 2026	Major version, published with Universal v3.0. Crypto-agility as the program's method read for digital asset organizations: the agility objective stated for the sector (an organization is crypto-agile when it can change the algorithm on its own custody stack, APIs and signing services on a planned date, and can name, per chain, the protocol change its on-chain keys wait on, that date's firmness grade and the address-rotation policy it applies meanwhile), the agility criterion and a rehearsal per wave on the custody stack, the APIs and the release-signing pipelines (a key ceremony that generates and retires a PQC-authorized signing key as the custody rehearsal; the quarterly HSM-partition failover recorded as a failover exercise whose timings do not feed the rehearsed time-to-change KPI), "migrated with agility debt" and the full delivery-state set of available, dependent and blocked applied to on-chain keys, with available used where the protocol capability and practical signer and verifier tooling both exist, and closure at zero unaccepted agility debt with protocol dependencies as SteerCo-signed exceptions. The shared-verifier-defect failure mode the Universal's Digital Assets note points to, written in Challenge 7 from OtterSec's disclosure of March 3, 2026 (six independent proof systems, one verifier defect) and cross-referenced to CCF layer 2, implementation lineage. The

Version	Date	Changes
		opening rebuilt on the 2026 resource-estimate sequence as the Universal's Activity 3.1 states it (Google Quantum AI, March; Schrottenloher, June; Luo et al., July; IonQ, September 3), adding the trapped-ion estimate to the Google figures rather than replacing them, with the June 2026 runtime corrected from nine minutes to the 18-minute wall-clock figure and the nine-minute primed-state window. Challenge 1 and Phase 1 inventory addresses under three separate records, observed exposure state read from the ledger at E1, reported key-control status at the grade of whoever reports it, and assessed migratability carried with its basis, with the Universal's wording that for most account models there is no re-key without moving the asset; Challenge 3 and Phase 7 state forged transactions as final once confirmed, qualified by protocol, and treat the protocol as a counterparty under Activity 7.6 with firmness grades on every protocol date; Challenge 8 cites the Federal Reserve Board staff working paper FEDS 2025-093 for the ledger-replica case under the paper's own disclaimer; Challenge 9 and Phase 6 state custody stacks as the migratable surface, with the four-field HSM, KMS and signing-stack register and entropy references, and nothing implying that HSM or multi-party custody changes the ledger's verification algorithm. The validation subsection rewritten to the per-product rule (CMVP certificate #5247, April 2026), correcting the June 2026 statement; the protocol-readiness paragraph re-verified line by line for September 2026 (Hegotá carrying EIP-8141 as scheduled for inclusion under the hardfork meta-EIP with no activation date set and no post-quantum scheme specified in the EIP itself; the Ethereum Foundation Protocol cluster's September 7, 2026 commitment to a quantum-resistant layer 1 by December 2029 superseding the June 27, 2026 assessment, graded announced because the firmness vocabulary reserves committed for contractual remedies; FN-DSA with no published date); three new alignment subsections (the agility criterion and rehearsal; evidence grades and the coverage denominator; vendor dates and questions). Phase adaptations mirror the v3.0 method: dual-outcome charter with named Crypto-Agility, Cryptographic Record and protocol-governance seats (Phase 0); exposure states, evidence grades and the enumerated denominator (Phase 1); the minimum record with the Profile as informative carriage, in three control classes (Phase 2); the sector's factors restated inside the Universal's dimensions with

Version	Date	Changes
		the arithmetic, Dimension 1 excluded for on-chain signing keys with the renormalized weights stated, the tier table re-derived from the Universal's ordered test with bridging patterns named for blocked Tier-1 entries, delivery state and the agility-debt register (Phase 3); the protocol timeline map with grades, the Re-Baseline Protocol and two results per gate record (Phase 4); the rehearsal per wave and the wave-exit criterion (Phase 5); the register (Phase 6); the protocol as a counterparty, the vendor classification by class, questionnaire order and the acceptance test (Phase 7). Regulatory content restructured under E1: the map rebuilt at four columns as a dated snapshot with MiCA and DORA as it reaches crypto-asset service providers, and the jurisdiction roster replaced by the Global PQC Migration Clock pointer. Exchange, custodian, wallet, audit-firm and HSM vendor names moved to Tool and Vendor References. Maturity supplement on the Universal's 0 to 5 scale; four agility KPIs with address-rotation coverage as the sector's own line; ten immediate actions. Requirements register generated as Appendix J. About block aligned to the Universal.

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 governance of decentralized protocols, which this edition treats as a counterparty the organization cannot compel. The Universal's Digital Assets note (Sector Adaptation Notes) is the binding summary: on-chain exposure by state, forged transactions final once confirmed, the protocol as a counterparty, custody stacks as the migratable surface. Readers should have the Universal Framework open alongside this document and cross-reference its phase definitions, maturity indicators, and templates.

WHAT'S NEW IN V3.0

Version 3.0 of the Digital Assets Extension publishes with Universal Framework v3.0 (September 2026). Crypto-agility is the program's organizing method and measured end state, and this extension states the ruling for the sector: an organization is crypto-agile when it can change the algorithm on its own custody stack, its own APIs and its own signing services on a planned date, and can name, per chain, the protocol change its on-chain keys wait on, the firmness grade of that change's date and the address-rotation policy it applies in the meantime; the agility criterion and

the rehearsal per wave run on the layer the organization controls, every on-chain key carries the delivery state its own facts give it, available where the protocol capability and the practical signer and verifier tooling both exist and dependent or blocked otherwise, shown with the dependency that unblocks it, and closure requires zero unaccepted agility debt with protocol dependencies as SteerCo-signed exceptions. Regulatory content states the mechanism and the two instruments that reach the sector; the jurisdiction roster is in the Universal's Regulatory Timeline Context and on the Global PQC Migration Clock page.

Content the Universal cites, and the 2026 estimate sequence. The shared-verifier-defect failure mode is written in Challenge 7, as the Universal's Digital Assets note says it is: on March 3, 2026 OtterSec disclosed that six independently developed proof systems and zkVMs had shipped one verifier defect (public-claim data not bound into the Fiat-Shamir transcript before challenge derivation), fixed between October 2025 and March 2026; the six shared a specification lineage rather than code, the defect has a patch path where a quantum break of the underlying assumptions has none, and the question of how many independent verifiers stand behind a portfolio of rollups is cross-referenced to the Cryptographic Concentration Framework at CCF layer 2, implementation lineage. The opening carries the 2026 resource-estimate sequence as the Universal's Activity 3.1 states it: Google Quantum AI in March (1,200 to 1,450 logical qubits on fewer than 500,000 superconducting qubits, about 18 minutes, nine from a primed state), Schrottenloher in June, Luo et al. in July, and IonQ on September 3 (1,457 logical qubits, 39 million Toffoli gates, 19,397 physical ions, 25.7 days per attempt, secp256k1-specific, with no P-256 or Ed25519 estimate at that depth), adding the trapped-ion figures to the Google estimate rather than replacing it.

Corrections made in the open. The June 2026 edition stated the Google runtime as roughly nine minutes; that is the primed-state figure, and the wall-clock runtime is about 18 minutes. It gave FN-DSA a publication window of late 2026 or early 2027; FIPS 206 is in development with no published date. It placed Ethereum's Hegotá hard fork in the second half of 2026; the ethereum.org roadmap targets 2027, and EIP-8141 is scheduled for inclusion under the hardfork meta-EIP EIP-8081 with no activation epoch or date set on any network. It stated that no FIPS 140-3 validated PQC module existed and treated validation as a calendar; that statement was wrong when published (CMVP certificate #5247, April 2026, ML-KEM at ML-KEM-768 and ML-KEM-1024 in a Level 1 software module; CMVP certificate #5497, August 2026, ML-KEM, ML-DSA, SLH-DSA and LMS inside the approved boundary of a Level 3 hardware module, each with the qualifications the validation subsection carries), and validation is decided per product, per operation and per certificate. It characterized the reception of BIP-361 as a community verdict; this edition states the proposal (assigned February 11, 2026, Draft) and the debate as dated facts, and discloses at the first substantive mention that one of the proposal's listed authors, Steve Vaile, is a Director of Applied Quantum. It structured the Phase 2 CBOM in three "layers", which collided with the Universal's CBOM Layers 1 to 4; they are three control classes. The named exchange in Challenge 9 is replaced by its class, with the name in Tool and Vendor References. It put post-quantum signatures at 30 to 60 times the size of the ECDSA signatures they replace, a range wrong at both ends and contradicted by the figures in the same paragraph; against the 64-byte signature they would replace, the four algorithms this extension names run from 10.4× to 122.8×. It called the cryptographic key the sole proof of ownership; a node verifies a signature or authorization witness and reads neither the private key nor legal title. It gave the Bitcoin block limit as 4 MB and a throughput reduction of roughly 60 percent for an ML-DSA-44 substitution; that was a units error, since BIP-141 sets the limit at 4,000,000 weight units and weights a witness byte at one against four for every other byte, and the corrected worked example in Challenge 2 gives a larger reduction than the published figure.

Alignment section, adaptations and supplements. The alignment section is rebuilt on v3.0, its validation subsection rewritten to the per-product rule and retitled, its protocol-readiness paragraph re-verified line by line for September 2026 with every claim dated (QRL since 2018; Algorand's first mainnet post-quantum transaction in November 2025, native Falcon-1024 accounts live on mainnet as of August 2026 with the v5.0.0 consensus upgrade, native rekey as the migration path and consensus still on an elliptic-curve VRF; Solana's Anza and Firedancer selecting Falcon, April 27, 2026; Zcash's Ironwood Quantum Recoverability (ZIP 2005) activated with NU6.3 on July 28, 2026, which the ZIP states is not by itself post-quantum security, and the 12-to-18-month Tachyon target from May 7, 2026; pq.ethereum.org from March 25, 2026, with the Ethereum Foundation Protocol cluster's September 7, 2026 cluster-wide commitment to a quantum-resistant layer 1 by December 2029 superseding the Post-Quantum team's June 27, 2026 assessment and graded announced; Bitcoin with no activated proposal), its closure subsection rewritten to the four dispositions, and three subsections added (the agility criterion and rehearsal; evidence grades and the coverage denominator; vendor dates and questions). Challenge 1 and Phase 1 inventory addresses under three separate records, observed exposure state read from the ledger at E1, reported key-control status at the grade of whoever reports it, and assessed migratability carried with its basis, with the Universal's wording that for most account models there is no re-key without moving the asset and Algorand's native rekey as the exception; Challenge 3 and Phase 7 state forged transactions as final once confirmed, qualified by protocol, and read each element of the Activity 7.6 counterparty pattern for a protocol; Challenge 8 cites the Federal Reserve Board staff working paper FEDS 2025-093 for the ledger-replica case, attributed as staff research under its own disclaimer; Challenge 9 and Phase 6 state custody stacks as the migratable surface with the four-field HSM, KMS and signing-stack register and entropy references, and nothing in either implies that HSM or multi-party custody changes the ledger's verification algorithm. The phase adaptations mirror the v3.0 method where this extension already adapts the element: the dual-outcome charter with named Crypto-Agility, Cryptographic Record and protocol-governance seats (Phase 0); exposure states, evidence grades and the denominator enumerated from the treasury and custody records before any scan (Phase 1); the minimum record with the Applied Quantum CBOM Profile as informative carriage (Phase 2); the sector's factors restated inside the Universal's dimensions with the arithmetic, Dimension 1 excluded for on-chain signing keys with the renormalized weights stated (TNFL and regulatory pressure tie at 38.46 percent), the tier table re-derived from the Universal's ordered test with every on-chain key in Tier 1 on verifier updatability (the factor scoped to the implementation that performs the verification, so enrolled customer passkeys are not placed by it and carry credential re-enrollment as their own recorded constraint) and bridging patterns named for blocked entries, delivery state and the agility-debt register with the on-chain population as its own line (Phase 3); the protocol timeline map with firmness grades, the Re-Baseline Protocol and two results per gate record (Phase 4); the rehearsal per wave and the wave-exit criterion (Phase 5); the register (Phase 6); the protocol as a counterparty, the vendor classification by class, the questionnaire order and the acceptance test (Phase 7). The regulatory map is rebuilt at four columns as a dated snapshot with MiCA and DORA as it reaches crypto-asset service providers (both in force, the transitional period closed on July 1, 2026), and the June edition's US, Asian and BIS/FSB rows not carried; the maturity supplement is re-based on the Universal's 0 to 5 scale with the on-chain and custody estates stated separately; the KPI supplement gains the four agility KPIs with address-rotation coverage as the sector's own line; ten immediate actions include naming the agility owner and scheduling the first rehearsal. Further Reading adds the IonQ analysis, the May 2026 chain-by-chain reading, the July 2026 HNDL analysis and the Global PQC Migration Clock; Appendix J lists the extension's own requirements.

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.

TOOL AND VENDOR REFERENCES

This framework references specific tools, products, and vendors as illustrative examples to help practitioners understand the categories of capability available. A mention does not constitute an endorsement, recommendation, or assessment of fitness for any particular environment. 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.

The body of this edition names categories and capability requirements. Commercial vendors appear in the body only where a dated public fact is itself the evidence (an announcement, a measurement, a published disclosure), and the counterparties a reader deals with regardless of choice (protocol foundations and client teams, standards bodies) are named as public facts. The six open-source proof systems named in Challenge 7 are named as the subject of a dated public disclosure and are not vendor references. The references below carry the names the body relied on in the June 2026 edition, as named there and verified September 2026 where a date is given, and are maintained on PQCFramework.org between editions.

Custodial and exchange platforms (Challenge 9; Phase 7): the June 2026 edition named Coinbase, Binance, Kraken, BitGo, Fireblocks and Anchorage as the custodial and exchange platforms a program engages. The 2026 position paper of Coinbase's Quantum Advisory Council on quantum computing and blockchain, analyzed on PostQuantum.com (Further Reading), is the industry signal Challenge 9 refers to. The list describes the market this extension was written against; it is not an assessment of any platform's PQC readiness, which is established per platform through the questionnaire in Phase 7 and graded for firmness.

Wallet software and hardware providers (Phase 7): the June 2026 edition named Ledger and Trezor (hardware wallets) and MetaMask, Phantom and Electrum (software wallets). The second agility question of Activity 7.2 decides each hardware wallet's class: whether the firmware verification key in devices already in the field can follow an algorithm change.

Smart contract audit firms (Phase 7): the June 2026 edition named Trail of Bits, OpenZeppelin, Certora and Consensys Diligence. The quantum vulnerability assessment and the verifier-lineage questions of Challenge 7 are asked of whichever firm the organization engages.

Multi-party and threshold signing providers (Phase 6; Phase 7): none named at the June 2026 edition; the register records the signing library and its version per stack, and the Cryptographic Concentration Framework answers whether two providers share one library.

General-purpose HSMs (Phase 6; Phase 7): the June 2026 edition named Thales, Utimaco, Futurex and Entrust. Thales Luna HSM firmware 7.9 (July 2025) added native ML-KEM and ML-DSA, with FIPS 140-3 Level 3 validation of that firmware in progress at release. Utimaco Quantum Protect (April 2025) is an application package for the u.trust General Purpose HSM Se-Series, activated in the field without a hardware exchange, carrying ML-KEM, ML-DSA, LMS/HSS and XMSS/XMSS-MT; older Utimaco models outside the Se-Series are a hardware question. Entrust nShield and Futurex product lines carry their own PQC firmware timelines, unverified at this edition. Validation is read per product from the CMVP list, never from a product name.

Cloud key management (Activity 6.2): AWS KMS, Azure Key Vault and Google Cloud KMS publish their own PQC key-type roadmaps; check the current status per service and region.

Validated modules (alignment section; Challenge 9): CMVP certificate #5247 (the Go Cryptographic Module, Geomys LLC, a FIPS 140-3 Level 1 software module validated April 27, 2026) lists ML-KEM key generation and encapsulation-decapsulation at ML-KEM-768 and ML-KEM-1024 only, with no ML-DSA; CMVP certificate #5497 (the QASM Cryptographic Module, Crypto4A Technologies, a FIPS 140-3 Level 3 hardware module validated August 19, 2026) lists ML-KEM, ML-DSA, SLH-DSA and LMS as approved algorithms, with the qualifications stated in the validation subsection. Some validated modules list PQC only among their non-approved services, and a listing of that kind does not count; a custody HSM is checked one product, one firmware family and one certificate at a time. Consult the CMVP validated-modules and Modules in Process lists for the current state.

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.org, a dedicated companion site for this framework, drawing on relevant content from PostQuantum.com.

Two sibling Applied Quantum properties carry work this framework cites rather than repeats. The Applied Quantum CBOM Profile, the property taxonomy layered on CycloneDX that Phase 2 cites by minimum version, publishes at CBOMProfile.org. The Cryptographic Concentration Framework, which measures cryptographic concentration beneath the vendor layer and consumes a Profile-conforming CBOM, publishes at CCFramework.org. Both are open under CC BY 4.0 and follow this framework's sector taxonomy.

This framework 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). Quantum Academy (QuantumAcademy.com), founded by the author, offers trainings and certifications on the topics this framework covers, for the roles and training levels described in Skills & Team Structure.

The PQC Migration Brief (pqcmigrationbrief.com) carries corrections, standards and regulatory movement between editions, and the current jurisdiction roster is maintained on the Global PQC Migration Clock page on PostQuantum.com; the framework itself remains free and ungated.

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 migration challenge: the protocol verifies an authorization witness, usually a signature, and not the private key and not legal title, so whoever can produce that witness moves the asset.

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 of the signature scheme a chain verifies requires consensus-level protocol changes across decentralized networks where no single entity has authority to mandate upgrades; moving a holding to an output type, account type or authorizer the chain already offers is a transaction the holder makes under the existing rules. Digital asset exposure is shaped by three distinct attack classes (on-spend, at-rest, and on-setup) that do not occur in enterprise cryptographic migration.

In 2026 the cost of the secp256k1 attack was re-estimated four times, each revision lowering the resource requirement, and a planner reads the trajectory rather than the last figure. Google Quantum AI's March whitepaper put a 256-bit-curve attack at 1,200

to 1,450 logical qubits depending on the gate budget, on fewer than 500,000 superconducting qubits, with the low-gate circuit running about 18 minutes, or about nine minutes from a primed state once a public key is revealed. The physical-qubit figure is roughly a 20-fold reduction against the prior best estimate for the curve (about 9 million on a photonic architecture, Litinski 2023).

Schrottenloher's June circuits (arXiv 2606.02235) reproduced it in the open at 1,462 logical qubits and about 58 million Toffoli gates for secp256k1. Luo et al. reached 835 logical qubits in July (arXiv 2607.13816) with a circuit that pays for its width in gates. IonQ's paper of September 3, 2026 compiled the secp256k1 attack to 1,457 logical qubits and 39 million Toffoli gates on a modeled trapped-ion machine of 19,397 physical ions at 25.7 days per attempt.

A March 2026 paper from Oratomic, Caltech and UC Berkeley (arXiv 2603.28627) put a comparable attack on P-256 at about 26,000 neutral atoms over a few days. The paper's ECC-256 estimates use Google's published circuit compilations, so the result is not an independent corroboration of the Google figure. No quantum computer at these scales has been built. No trapped-ion estimate at the depth of IonQ's secp256k1 compilation exists for P-256 or Ed25519 (Universal, Activity 3.1). The assumption ledger behind each 2026 result is analyzed on PostQuantum.com (Further Reading).

For this extension the sequence changes the attacker's horizon in two directions. A minutes-scale machine makes the on-spend attack thinkable against a ten-minute block interval. A machine that needs weeks per key cannot execute the on-spend attack. It can instead derive the private key from every public key that has been visible on-chain for weeks – the at-rest population Challenge 1 inventories by exposure state.

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, what the protocol verifies is an authorization witness, usually a signature; legal title is settled off-chain and the protocol does not read it.

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 produce the witness the protocol accepts and transfer the asset to themselves, and the base layer offers no native reversal. This makes every exposed public key on a base-layer chain a potential quantum theft target whose payout is the value the key controls, less whatever an issuer's freeze role, a permissioned operator or an off-chain remedy can block at the asset layer (Challenge 3).

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 proposal track, Ethereum's EIP workflow, and each alternative chain's governance model impose their own coordination costs, political dynamics, and implementation timelines.

BIP-361 (Lopp, Papathanasiou, Smith, Ross, Vaile and Dallaire-Demers; BIP number assigned February 11, 2026; an Informational BIP in Draft status, not activated) proposes a legacy-signature sunset under which unmigrated coins become unspendable after a dated phase, and the proposal opened a governance debate on whether protection from a future attacker justifies freezing present holders. Steve Vaile, a Director of Applied Quantum, is one of BIP-361's six listed authors. This extension cites the proposal as external and states the debate around it as third-party fact, with that connection disclosed.

The engineering for a PQC migration exists; whether decentralized governance can coordinate action against a time-bounded threat is the open question, and this extension treats each protocol's governance as a counterparty the organization cannot compel (Universal, Activity 7.6).

On-Spend, At-Rest and On-Setup Attack Classes

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 compute private keys from public keys already exposed on-chain and require only a patient quantum computer with unlimited time. On-setup attacks extract the secret values generated during a zero-knowledge proof system's trusted setup ceremony; once obtained, those values yield a reusable classical exploit with no further quantum access required.

Enterprises meet versions of the first two classes: certificates and code-signing chains expose long-lived public keys, and cryptographic proof setups appear in enterprise systems too. What is distinctive here is the combination. The exposed key authorizes value directly, the exposure is published to everyone and stays published, and the remediation runs through a governance process the holder does not control.

Irreversible Losses and Unmigrable Assets

BIP-361 states that as of March 1, 2026 over 34% of all bitcoin had revealed a public key on-chain. Google Quantum AI's March 2026 whitepaper puts the Satoshi-era pay-to-

public-key population at over 1.7 million BTC. The figure is an estimate of coins that have not moved since they were created. The ledger shows the dormancy and nothing about key control. The population is carried as dormant, with owner and key-control status unknown.

A still-held key can spend those coins until an attacker derives it, and a key nobody holds can never migrate them. The June 2026 edition of this extension recorded the exposed population as approximately 6.7 million BTC on the same basis. Privacy-preserving blockchains face retroactive deanonymization: a quantum computer could decrypt years of historical shielded Zcash transactions for addresses whose public keys it holds, even after the protocol migrates to PQC.

No future migration can undo past exposure. Re-encrypting enterprise data at rest does not repair a historical exposure either; what differs is reach and permanence. A public ledger publishes the historical ciphertext to everyone and every full node keeps it, while an enterprise operator still controls the copies an attacker has not taken and everything written from now on.

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. Most account models offer no in-place credential rotation (Universal, Digital Assets note): a legacy EOA is permanently bound to its original signing pair, so reducing exposure requires moving assets to a fresh account or adopting account-abstraction mechanisms where available. The exception is a protocol with a native rekey, such as Algorand's, which lets an account change its authorizing key without changing its address. Where the protocol offers one, the inventory records it as the migration path.

The organization therefore inventories every address, account and contract it controls or depends on under three records, kept apart because they do not rest on the same evidence. The observed exposure state is read from the ledger and grades E1 (Universal, Activity 1.2): no exposure observed in the assessed sources (a hash-protected output, never spent from, never reused); exposed by format (P2PK; a P2TR key path; any account model that publishes the key); or exposed by history (spent from, reused, or an EOA that has sent).

The reported key-control status takes the grade of whoever reports it: controlled, on the custody record that says so; or dormant, with owner and key-control status unknown, which is where a holding stays unless loss is established independently of the chain.

Assessed migratability is a judgment recorded with its basis: migratable under the protocol as it stands, migratable only after a protocol change, or not established. The ledger shows script or account format, transactions and dormancy.

It cannot show that an owner lost a key. Nor can it show that a public key was never exposed off-chain, through an extended public key, or in an unconfirmed transaction. The first record is scoped to the sources actually assessed. The value at risk is recorded with the three, in units of the asset and, where a fiat figure is needed, with a dated price assumption.

This creates an at-rest attack surface measured in trillions of dollars. A quantum attacker with a patient machine (even one requiring days or weeks per key derivation, the shape of the September 2026 trapped-ion estimate) could methodically work through exposed high-value addresses. The exposed share of Bitcoin's supply, over 34% as of March 1, 2026 per BIP-361, is a material fraction of the asset. 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 (Google Quantum AI, March 2026).

Framework Impact: Phase 1 (Discovery) must include on-chain public key exposure analysis as a primary inventory track. Phase 1 must record it as three separate claims: observed exposure state, reported key-control status and assessed migratability. Phase 3 (Risk Scoring) must weight at-rest exposure by value concentration and key recovery feasibility, reading the observed exposure state and the value at risk as factors inside Dimension 2 (Phase 3 adaptation).

Challenge 2: Signature Size and Transaction Throughput

Blockchain transaction throughput is directly constrained by block size or gas limits. Post-quantum signatures run roughly one to two orders of magnitude larger than the 64-byte Schnorr signature (BIP-340) of a Taproot key-path spend on secp256k1, Bitcoin's curve, which they would replace:

- ML-DSA-44 at 2,420 bytes, a 37.8× increase.
- ML-DSA-87 at 4,627 bytes, about 72×.
- SLH-DSA at security level 1, 7,856 bytes, 122.8×.
- FN-DSA-512 at 666 bytes, 10.4×.

Bitcoin's block limit is 4,000,000 weight units under BIP-141's accounting, in which a witness byte counts one unit and every other byte four, so the effect on throughput does not follow from the signature-size ratio alone. On one stated illustrative basis, a one-input, two-output Taproot key-path transaction of about 616 weight units (154 virtual bytes) whose only witness item is the 64-byte signature, replacing that signature with a 2,420-byte ML-DSA-44 signature raises the transaction to about 2,970 weight units,

roughly 4.8 times its size, so a block filled with such transactions holds about one fifth as many. A 7,856-byte SLH-DSA signature at security level 1 raises it to about 8,400 weight units, roughly 13.7 times.

Those figures are arithmetic on the stated assumptions and not a measured result. A different script path, a batching or aggregation design, or a signature-aggregation proposal changes them, and the Phase 5 modeling measures the organization's own transaction mix.

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 validator client teams, Anza and Firedancer, independently selected Falcon and published initial implementations (Solana Foundation, April 27, 2026). However, FN-DSA's implementation complexity (floating-point arithmetic in signing, trapdoor sampling) and its later NIST standardization timeline have slowed adoption.

NIST selected Falcon for standardization as FN-DSA (FIPS 206). The standard is in development with no published date at this edition (Universal, Appendix A), so a chain that adopts Falcon now adopts a pre-standard parameter set and records the dependency. 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. Introducing a post-quantum signature scheme or a new output type on a chain requires the chain's own activation and enforcement process, together with adoption by the participants that need the new function; moving a holding to an authorizer or output type the chain already offers does not. Three things are distinct, and the record keeps them apart. A soft fork tightens validation rules, so nodes running the older software keep accepting blocks produced under the new ones.

A hard fork produces blocks those nodes reject. A holder action is taken under rules the chain already enforces. Activation, enforcement by the validating population, signer support and wallet adoption are four populations on four schedules. A chain can have activated a rule that most wallets cannot yet produce a transaction for. For Bitcoin, a consensus change means a soft fork or a hard fork activated through miner and node signaling.

BIP-360 (BIP number assigned December 18, 2024; renamed Pay-to-Merkle-Root, P2MR, on February 10, 2026; current revision July 24, 2026; a Consensus soft-fork specification in Draft status) proposes a new output type whose spending paths are script paths only, removing the quantum-vulnerable key path of Taproot. The BIP states that it does not include post-quantum signature schemes: P2MR reduces exposure to long-exposure attacks on public keys visible on-chain and is not a post-quantum output type, and the authors intend to propose post-quantum signatures separately.

BIP-361 (assigned February 11, 2026; Informational, Draft) proposes a phased legacy-signature sunset after a post-quantum output type exists, which no assigned BIP yet defines. 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. As of September 2026 neither proposal has been activated and neither carries an activation date.

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 Transaction, native account abstraction enabling signature agility) is scheduled for inclusion in the Hegotá hard fork.

The hardfork meta-EIP, EIP-8081, is the formal record of what Hegotá includes, and its Scheduled for Inclusion list holds exactly two entries, EIP-7805 (FOCIL) and EIP-8141. Its Considered and Declined lists were both empty when the meta-EIP was read on September 14, 2026. The specification is still Draft, and no activation epoch or date is set on any network: the meta-EIP's activation table has rows for Sepolia, Hoodi and mainnet with every epoch and timestamp field blank.

The 2027 target for Hegotá comes from the ethereum.org roadmap rather than from the meta-EIP. The June 2026 edition of this extension placed Hegotá in the second half of 2026. Any statement about what Hegotá includes or declines is read from EIP-8081 and not from the Protocol cluster's graded tier-list commentary.

EIP-8141 is the mechanism for signature agility, not a post-quantum signature scheme, and this extension draws that line as it draws it for BIP-360. The EIP defines three protocol-validated signature schemes, ARBITRARY (0x0), SECP256K1 (0x1) and P256 (0x2), and reserves 0x3 through 255. No post-quantum scheme is specified. A post-quantum scheme reaches an account either through an ARBITRARY entry whose witness is verified by contract code running in the EVM, or through a scheme number assigned later. The state-backed alias that would carry large public keys is described in the EIP's rationale as a future extension.

Frame Transaction also does not retire secp256k1 on its own. The Ethereum Foundation Protocol cluster names EIP-8298 (SETCODEFROM) and EIP-8151 as the pair forming the

account path for retiring secp256k1 as a master key. It names EIP-8365 (BLS Withdrawal Credential Retirement) as the start of retiring withdrawal credentials tied to vulnerable cryptography. None of those three is scheduled for inclusion in Hegotá.

The Ethereum Foundation launched pq.ethereum.org on March 25, 2026, with more than ten client teams running weekly post-quantum interoperability devnets. On September 7, 2026 its Protocol cluster published a cluster-wide commitment to make Ethereum layer 1 quantum-resistant across execution, consensus and data by December 2029, which supersedes the Post-Quantum team's June 27, 2026 assessment that layer-1 upgrades could complete by 2029 (Phase 4 adaptation states the milestones and the firmness grade). 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. Two consequences follow for the program. First, a transaction signed with a forged key is final once confirmed, qualified by protocol. On Bitcoin's and Ethereum's base layers there is no reversal, while an issuer's freeze or blacklist role, a permissioned ledger's operator, or an off-chain legal remedy can block or unwind at the asset layer.

That recovery is a governance remedy, not a cryptographic one. The organization records per asset which remedy exists (Universal, Digital Assets note). Second, the protocol is treated as a counterparty under the pattern of Activity 7.6: its PQC posture is read from the ledger and the proposal record rather than from a questionnaire, every roadmap date it publishes has a firmness grade, and the refusal decision is taken for the chain whose governance will not move (Phase 4 and Phase 7 adaptations).

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, each graded for firmness, with the dependent on-chain entries shown against the dates that unblock them.

Challenge 4: Unmigrable Assets and Dormant Coins

Over 1.7 million BTC in Satoshi-era P2PK scripts (Google Quantum AI, March 2026) have permanently exposed public keys and have not moved since the era in which they were created. The private keys are presumed lost on that dormancy, which the ledger shows, and not on loss, which it cannot establish. 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 sunset legacy signatures after a grace period, which would leave such coins unspendable, opened a governance debate between security and the immutability principle that was unresolved as of September 2026.

This creates a risk for every participant, not only the holder: 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 are targets where a key that holds little ETH controls a large amount of value, and a single compromised key can trigger cascading damage. Hundreds of billions of dollars in stablecoins and tokenized real-world assets are controlled by 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. That dependency now has a number. EIP-8355, precompiles for ML-DSA verification, is listed at Proposed for Inclusion in EIP-8081 and is not scheduled, so it grades unknown, and the entries waiting on it stay blocked and are shown against it on the record (Phase 4 adaptation).

Whether a contract can upgrade its cryptographic dependencies is recorded field by field rather than read off a pattern name, because a timelock delays an authorized operation and does not by itself make the code immutable or the verifier fixed. Record, for each contract the organization depends on: whether the code is immutable; who holds the upgrade authority; what delay applies; which cryptographic dependencies are external to the contract; and whether replacement verification logic is available. A contract whose code is immutable and whose verification path runs through a hardcoded precompile is the case that cannot be upgraded at all.

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. At the June 2026 edition approximately 36 million ETH was staked across roughly 1.1 million validators (Google Quantum AI's March 2026 whitepaper counts about 37 million ETH in the consensus exposure). 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).

Bitcoin's Proof-of-Work 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. The Ethereum Foundation's consensus-layer plan replaces BLS with hash-based validator signatures (leanXMSS) with SNARK-based aggregation to restore scalability (pq.ethereum.org, June 27, 2026).

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 (Groth16 over BLS12-381 with a trusted setup) falls in the same on-setup class – an undetected-inflation exploit for that pool. Orchard (2022) removed the trusted setup with Halo 2 but remains quantum-vulnerable on its curve

assumptions. Zcash's roadmap treats the Sprout, Sapling and Orchard pools as legacy behind the Ironwood pool (Phase 4 adaptation). Any ZK proof system built on pairing-based curves with a trusted setup shares the on-setup vulnerability class.

Mimblewimble Pedersen commitments use transparent generators rather than 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 one 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.

A verifier defect shared across independent implementations is a third failure mode, alongside the algorithmic break and the single-implementation bug, and the Universal's Digital Assets note points here for its treatment. On March 3, 2026 OtterSec disclosed that six independently developed proof systems and zkVMs (Jolt, Nexus, Cairo-M, Ceno, Expander and Binius64) had shipped one verifier defect: prover-controlled public-claim data was not bound into the Fiat-Shamir transcript before the challenges were derived, so a prover could choose those values after seeing the challenges and pass verification of a false statement.

The teams were notified between September and December 2025 and the fixes shipped between October 3, 2025 and March 5, 2026 (OtterSec, "Unfaithful claims: breaking 6 zkVMs", https://osec.io/blog/zkvms-unfaithful-claims/). The six shared no code. They shared a lineage: the academic specifications describe the interactive protocol and leave the transcript binding to the implementer. All six made the same omission. That is the shared-verifier-defect failure mode, and it differs from the other two in its remedy.

An implementation defect has a patch path, one or two lines per system. The patch restores soundness. A quantum break of the underlying assumptions (the discrete logarithm on the pairing curve, the recovered toxic waste) has no patch path. The recovered parameters remain valid indefinitely. A shared defect has a patch path per implementation. Implementation diversity gave no assurance against this one: the six verifiers that appeared independent failed together on an omission their shared specifications left to the implementer.

The finding establishes that a specification-level defect crosses implementations. It does not establish that implementation diversity has no value against an implementation-level bug, which stays inside the implementation that has it. Record each proof system the organization depends on (rollups, bridges, privacy pools) with its specification lineage and its verifier implementation. Treat the question of how many independent verifier implementations actually stand behind a portfolio of rollups as a

Cryptographic Concentration Framework question at CCF layer 2, implementation lineage, cross-referenced from the Phase 3 scoring and not recomputed here.

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. Phase 7 (Vendor Governance) must ask every rollup, bridge and proof-system provider which specification its verifier implements, whether the transcript binding of every prover-supplied value has been reviewed against that specification, and which other deployed verifiers share the lineage.

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 whose public keys the attacker holds; recipient keys are not on the chain, the ephemeral keys are, so the exposure is per known address rather than for the whole pool. 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 case of Harvest Now, Decrypt Later (HNDL). The framework's position is stated in the Universal: HNDL is planned on as inference from demonstrated capability (means, motive, opportunity, precedent), never on observed harvesting, and a passive collector leaves no trace. On a public ledger every full node already stores a complete copy of the data an attacker would harvest. A Federal Reserve Board staff working paper (Mascelli, J., and M.

Rodden (2025), "Harvest Now Decrypt Later": Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks, Finance and Economics Discussion Series 2025-093, Board of Governors of the Federal Reserve System, https://doi.org/10.17016/FEDS.2025.093) treats the ledger-replica case: a harvested replica of a public ledger is decrypted later regardless of any migration the network completes, and no privacy mitigation exists for transactions already recorded.

The paper describes HNDL as "a present, active, and in some circumstances unavoidable data privacy risk". It states that the views are the authors' and not those of the Board of Governors, the Federal Reserve Bank of Chicago or the Federal Reserve System, and this extension cites it as staff research on that basis. Re-encrypting stored data repairs no exposure that has already happened, in either setting. What an enterprise operator keeps is control over the copies an attacker has not taken and over everything written from now on.

A public ledger gives up both: the historical ciphertext is published to everyone, every full node keeps it, and the privacy guarantees users relied on when transacting become retroactively void. The reasoning for why a harvest cannot be detected, written for the funding conversation, is in the July 2026 PostQuantum.com analysis.

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.

Custodial key management, HSM-backed and multi-party signing stacks are the migratable surface today (Universal, Digital Assets note): the organization controls the key generation, the storage, the approval workflow and the transport around the signing operation, and can move each of them to validated modules, PQC-protected key wrapping, PQC-authenticated approvals and hybrid TLS now, on its own schedule.

What none of that changes is the signature the ledger verifies. An HSM or a multi-party (MPC, threshold) signing stack that holds a secp256k1 or Ed25519 key still produces a secp256k1 or Ed25519 signature. The protocol sets the verification algorithm. A custody migration therefore protects the key from theft through the stack but does not protect the exposed public key from a discrete-logarithm attack. The custody stack and the on-chain key are two entries in the inventory with two delivery states (Phase 1 and Phase 3 adaptations).

A 2026 position paper from a US-listed exchange's quantum advisory council (the exchange is named in Tool and Vendor References; the paper is analyzed on PostQuantum.com, Further Reading) recommended prioritizing HSM and KMS upgrades, implementing crypto-agility in signing infrastructure, and establishing quantum readiness metrics. As an industry signal it is consistent with this extension for the custodial surface. It does not address the on-chain exposure of customer funds in UTXO-based systems or the smart contract dependencies in DeFi. Those are treated in Challenges 1, 4 and 5.

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), as separate entries. Phase 6 (Infrastructure) must record every custodial HSM, KMS and multi-party signing stack in the four-field register with its entropy references. Phase 7 (Vendor Governance) must include blockchain node software providers, wallet SDKs and multi-party signing providers, agility questions first.

Challenge 10: Tokenized Real-World Assets and Stablecoins

The tokenized asset market (projected by Citi, in a forecast the June 2026 edition cited, 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 are held in smart contracts secured by the same quantum-vulnerable elliptic curve cryptography as native chain assets.

Stablecoins (USDT, USDC, DAI, and others) represented over $300 billion in aggregate market capitalization at the June 2026 edition, 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 protocol verifies an authorization witness and does not read legal title, so recovery after a chain compromise runs on the issuer's own controls and on the law governing the instrument rather than on the chain.

Those routes are recorded per asset, and where none is established that absence is itself the finding. 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 V3.0

Universal Framework v3.0 (September 2026) is a major version. Readiness against dated obligations is the mandate; crypto-agility is the method. The PQC migration is the first exercise of a standing capability. For organizations holding, custodying or building on digital assets the version changes the method, the records and the vendor governance, and corrects positions the June 2026 edition published.

- **Method.** The charter states both outcomes (Phase 0). The program runs ten workstreams, with Discovery separated from the permanent Cryptographic Record and Crypto-Agility funded from Year 1 (Activity 0.3). Every migration gate and wave exit applies the agility criterion, and a system whose algorithm cannot be changed by configuration and rehearsed with rollback is recorded as migrated with agility debt rather than as migrated (Activities 4.6 and 5.4).

Every wave carries an algorithm-change rehearsal (Activity 5.2). Closure requires a rehearsed second algorithm change per track inside the agility window (the 48-hour assessment plus the organization's change window, ten business days by default) and zero unaccepted agility debt (Migration Verification & Program Closure). Phase 3 produces an agility-debt register, and in this sector its largest population is on-chain: every key whose algorithm the protocol sets.

- **Records and evidence.** Every discovery finding receives an evidence grade E1 to E5; coverage is measured against a denominator enumerated before discovery ran. The accepted-gaps register is signed at gate G1 → G2 (Activity 1.2). The CBOM minimum record is the Universal's own (Activity 2.1), with the Applied Quantum CBOM Profile v1.0-RC or later cited as informative carriage and never required. The Cryptographic Concentration Framework is cross-referenced where the question is how many distinct implementations, firmware families or verifier lineages execute beneath the vendors and protocols an entry depends on (Activity 3.1; Challenge 7), and no concentration figure is computed in this extension.

- **Vendor governance.** Every roadmap date is graded for firmness (committed, forecast, announced, unknown). The questionnaire opens with the two agility questions and the firmness question; the four certificate-authority questions, the non-standardized-algorithm rule with its one-afternoon test, the provider-roadmap reading rule and the counterparty pattern apply (Activities 7.2, 7.3, 7.5, 7.6 and 7.7). In digital assets the counterparty pattern reaches its extreme case. The protocol whose signature algorithm the organization cannot set is a counterparty no participant can compel. This extension reads Activity 7.6 for it in Phase 7.
- **Corrections made in the open.**

On the Google Quantum AI runtime. The June 2026 edition stated the March 2026 runtime as roughly nine minutes. That is the primed-state figure for the low-gate circuit. The wall-clock runtime is about 18 minutes, and the opening states both.

On FN-DSA. It gave FN-DSA a publication window of late 2026 or early 2027. FIPS 206 is in development with no published date.

On the Hegotá hard fork. It placed the fork in the second half of 2026. The ethereum.org roadmap targets 2027, and EIP-8141 is scheduled for inclusion under the hardfork meta-EIP with no activation date set on any network.

On validated modules. It stated that no FIPS 140-3 validated PQC module existed, and treated validation as a calendar. That statement was wrong when published. CMVP certificate #5247 (April 2026) covers ML-KEM at ML-KEM-768 and ML-KEM-1024 in a Level 1 software module. CMVP certificate #5497 (August 2026) covers ML-KEM, ML-DSA, SLH-DSA and LMS inside the approved boundary of a Level 3 hardware module. Each comes with the qualifications the validation subsection states. Validation is decided per product, per operation and per certificate.

On BIP-361. It described the reception of the proposal as a community verdict. This edition states the proposal and the debate as facts with dates, with the Applied Quantum connection to one of the proposal's authors disclosed where the proposal is first discussed.

On CBOM structure. It structured the Phase 2 CBOM in three "layers", which collided with the Universal's CBOM Layers 1 to 4. They are three control classes here.

On signature sizes, it said that post-quantum signatures are "30 to 60 times larger than the ECDSA signatures they replace".

The range was wrong at both ends, and it contradicted the figures in its own paragraph. Against the 64-byte signature they would replace, ML-DSA-44 at 2,420 bytes is 37.8×, ML-DSA-87 at 4,627 bytes about 72×, SLH-DSA at security level 1 at 7,856 bytes 122.8×, and FN-DSA-512 at 666 bytes 10.4×. The signature sizes in FIPS 204 and FIPS 205, and the Falcon specification for FN-DSA-512, settle it. Challenge 2 states all four.

On ownership, it said that in blockchain systems "the cryptographic key is the sole proof of ownership".

A node verifies a signature or authorization witness against the output, account or script. It reads neither the private key nor legal title, which is settled off-chain. The chains' own verification rules settle it. The distinctive issue is protocol-level authorization, public exposure and governance-dependent remediation, which is how the opening section and Challenge 3 now state it.

On block throughput, it said that "Bitcoin's 4 MB SegWit block weight limit would accommodate roughly 60% fewer transactions if every signature were replaced with ML-DSA-44", and repeated the 60 percent figure in its hybrid-signature discussion.

That was a units error. BIP-141 sets the limit at 4,000,000 weight units rather than 4 MB, and weights a witness byte at one unit against four for every other byte, so no throughput figure follows from a signature-size ratio alone. A reader who sized throughput impact from the published figure should redo it in weight units on their own transaction mix. The corrected worked example in Challenge 2 shows what the arithmetic gives on one stated illustrative basis: about 4.8 times the weight for an ML-DSA-44 substitution and roughly one fifth as many transactions per block, a larger reduction than the published figure.

Standards currency runs to September 2026: RFC 9954 and RFC 10024 for hybrid key establishment in TLS, which exchange and custody APIs and wallet-to-node RPC read; RFC 10042 for hybrid key establishment in SSH on node and validator management access; RFC 9964 for ML-DSA in JOSE and COSE, which API request signing and token signing read; FIPS 206 (FN-DSA) in development with no date; and the section 8 conditions of SP 800-208 on the deploy-now signing action.

The subsections below read each element for digital asset organizations. The last three read elements the June 2026 edition did not cover (the agility criterion and rehearsal; evidence grades and the coverage denominator; vendor dates and questions). The remaining Universal positions (the stored-data strategy decision 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 and the Re-Baseline Protocol in 4.8, the risk-weighted coverage KPI, algorithm sovereignty and standards fragmentation, crisis communications, the skills matrix, and Appendices G, H and I) apply as written, with two notes.

The stored-data strategy of Activity 5.6 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 subsection in this section and by Challenge 8. The counterparty coordination pattern of 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 Phase 4 and Phase 7 adaptations are 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 and the polynomial commitments beneath them (Groth16; KZG), and code-signing for node software releases. Adding a post-quantum signature scheme or output type to a chain requires a consensus change that no organization can make unilaterally. Where a chain already offers a post-quantum authorizer (Algorand's native Falcon-1024 accounts and its rekey) or contract-level validation logic under account abstraction, the organization moves its own keys under the existing rules, and that move is available rather than dependent.

Rotation to a hash-protected output is not a universal option. Chains differ in their address and authorization models: a Bitcoin holding can move to a never-spent-from hash-protected output, while an ordinary Solana keypair account's address is the public key itself. No hash-protected form of that account exists, and a program-derived address is a different authorization construction rather than a substitute for one. Hash-protected rotation is offered only where the chain's address model and the holding's own spending requirements support it, on the per-chain record the address-rotation policy carries (Phase 5 adaptation).

The difference from enterprise migration is who decides: 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. An on-chain Track B entry takes the delivery state its own facts give it (Phase 3 adaptation): available where the protocol capability and the practical signer and verifier tooling both exist, dependent where an identified external delivery is still required, and blocked where no feasible approved path exists.

Chain-wide consensus risk is recorded separately from the holder's own migration, which is an action the organization can schedule and take. The Universal's default weights (HNDL 0.35, TNFL 0.25) stand for the custody estate, ratified by the SteerCo before the first scoring run. For an on-chain signing key that protects no confidentiality, Dimension 1 does not apply and is excluded with the weights renormalized under the

Universal's arithmetic (Activity 3.2): 0.25 / 0.65 = 38.46 percent for TNFL, 38.46 percent for regulatory pressure and 0.15 / 0.65 = 23.08 percent for feasibility.

TNFL and regulatory pressure tie. TNFL leads the composite only where the regulatory dimension scores lower on that entry, which is a fact about the entry and not about the arithmetic. The Universal's Digital Assets note states TNFL as the primary threat, a threat-priority statement the sector reads through the ordered tier test of Activity 3.2 and not through the weights. No sector weight set is added.

Validation Decided Per Product, Per Operation, Per Certificate in Custody

Regulated custodial platforms and exchanges operating in jurisdictions or under contracts that require FIPS-validated cryptography check the obligation at its source. Never assume it from the sector, and plan it per product.

The June 2026 edition stated that no FIPS 140-3 validated PQC module existed, and that the absence constrained production HSM deployment for custodial key management as a calendar. That statement was wrong when published. As of September 2026 the CMVP validated-modules list includes post-quantum operations as approved services in software and in hardware, and the two certificates this extension cites are not interchangeable evidence. Validation is decided per product, per operation and per certificate (Universal, Deployment Environment Classification).

Property	Certificate #5247	Certificate #5497
Module	Go Cryptographic Module (versions v1.0.0 and v1.0.1, Geomys LLC)	QASM Cryptographic Module (Crypto4A Technologies, hardware version QASM 1.1, firmware 5.0.1.158)
Type and level	FIPS 140-3 Level 1 software module	FIPS 140-3 Level 3 multi-chip standalone hardware module
Dates	Validated April 27, 2026; updated July 7, 2026	Initially validated August 19, 2026; updated August 21, 2026; sunset date August 18, 2031
ML-KEM	KeyGen and EncapDecap, which covers encapsulation and decapsulation, at ML-KEM-768 and ML-KEM-1024 only, not ML-KEM-512	KeyGen and EncapDecap at ML-KEM-512, -768 and -1024
ML-DSA	None. The Go module version	KeyGen, SigGen and SigVer at

Property	Certificate #5247	Certificate #5497
	that implements ML-DSA is on the Modules in Process list, not on the validated list	ML-DSA-44, -65 and -87
Other approved algorithms	Not applicable	SLH-DSA across all twelve parameter sets, and LMS

Two qualifications from #5497's Security Policy apply to every citation of it. The first is that §2.7 states that the module does not establish SSPs using an approved KEM, and instead exposes ML-KEM functionality for an external application to use as part of an approved KEM. The second is that HSS key generation, signing and verification are vendor-affirmed, not CAVP-tested.

A sentence asserting that approved post-quantum key establishment exists in a validated module cites one certificate with its qualification (#5247 with its parameter-set limit, #5497 with its §2.7 statement), never both as a single proposition. Every ML-DSA statement in this extension cites #5497 alone. A module that lists PQC only among its non-approved services does not count.

For each FIPS-required custody deployment, record:

- the governing requirement
- the exact module and version
- the certificate number and status
- the approved services the certificate lists
- the required security level
- the tested operating environment

Confirm that the intended operation is covered. Where no validated product covers a custody operation, record the dependency with the vendor's evidence, the interim controls, the exception authority and the next decision date. It constrains that system and sets no date for the program.

Sequence the rollout in three steps:

1. **Pilots**, now, in unrestricted environments.
2. **FIPS-aware systems**, with documented risk acceptance on CAVP-tested algorithms.
3. **FIPS-required production**, last, per system on the certificate date of the module that covers it, planned, staged and rehearsed in advance.

The certificate date is then only a change window.

Unregulated and DeFi-native operations typically face no FIPS requirement. The same estate can therefore run a FIPS-required cold-storage HSM and an unrestricted hot-wallet signer, and the classification is recorded per deployment. None of it touches the on-chain signature algorithm, which the protocol sets.

Protocol PQC Readiness by Chain, as of September 2026

Chain-by-chain readiness, checked for this edition, ranges from post-quantum by design to no activated proposal.

- **Quantum Resistant Ledger (QRL).** Has run hash-based (XMSS) signatures since its 2018 mainnet launch.
- **Algorand.** Has signed its state proofs with Falcon since 2022, and executed its first post-quantum transaction on mainnet in November 2025 through a Falcon-based account authorizer, with the protocol's native rekey as the account migration path (Algorand technical brief, June 1, 2026). With the v5.0.0 consensus upgrade (go-algorand v5.0.0-stable, released August 12, 2026) native Falcon-1024 account signatures are live on mainnet as of August 2026, with no LogicSig wrapper required, alongside post-quantum delegated LogicSigs and the algokey pq key-management commands. Ed25519 accounts remain supported.

Its consensus is not post-quantum. The Algorand Foundation's post-quantum page states that the verifiable random function driving consensus derives its guarantees from elliptic-curve cryptography, with a post-quantum VRF and consensus signatures as roadmap items targeting broad quantum resilience by the end of 2027, and post-quantum multisig a later milestone.

- **Solana.** Its two validator client teams, Anza and Firedancer, independently selected Falcon and published initial implementations. The Solana Foundation's phased plan states that no protocol change is required today (April 27, 2026).
- **Zcash.** ZIP 2005, Ironwood Quantum Recoverability, activated on mainnet with the NU6.3 network upgrade on July 28, 2026, at block 3,428,143 under ZIP 258, which also deploys the Orchard-to-Ironwood migration of ZIP 318. The June 2026 edition recorded it as a forecast, announced May 7, 2026 under the name Orchard quantum recoverability, of wallets shipping within a month.

The ZIP states in its own abstract that it does not by itself make the protocol secure against quantum adversaries. Recoverability is a migration step toward a future post-quantum version and not post-quantum security, and funds left in the Sprout, Sapling or Orchard pools become inaccessible once those protocols are disabled and move to the Ironwood pool to gain it.

The upgrade shipped in response to a soundness flaw in Orchard's proof circuit that Taylor Hornby discovered on May 29, 2026, the day ZIP 257 was created, and that was publicly disclosed on June 4, 2026, with quantum recoverability alongside it. Full post-

quantum status was targeted, at the May 7, 2026 announcement, within 12 to 18 months through Project Tachyon, a 2027 target. Zcash is not post-quantum today.

- **Ethereum.** The Ethereum Foundation launched pq.ethereum.org on March 25, 2026 with more than ten client teams on weekly interoperability devnets. Its Post-Quantum team assesses that layer-1 upgrades could complete by 2029, with execution-layer migration taking additional years (June 27, 2026).
- **Bitcoin.** No activated PQC proposal as of September 2026. BIP-360 (assigned December 18, 2024; P2MR since February 10, 2026; Draft) removes Taproot's key path without adding a post-quantum signature scheme. BIP-361 (assigned February 11, 2026; Draft) waits on a post-quantum output type no assigned BIP yet defines. Neither has an activation date.

Every claim above is dated because each will move. The chain-by-chain state between editions is maintained in the PostQuantum.com series in Further Reading. Organizations assess readiness chain by chain rather than assuming progress across the sector.

Hybrid and Composite Signatures on the Control Boundary

The Universal takes the position (Activity 5.2) 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.

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 ML-DSA, which on the illustrative basis stated in Challenge 2 already multiplies a Taproot key-path transaction's weight by about 4.8. Compactness therefore drives blockchain algorithm selection (FN-DSA), and composite schemes are unlikely on-chain.

Organizations cannot record a risk decision for a protocol they do not control, but they document the gap (which holdings depend on chains with solo-PQC or no-PQC trajectories) as an accepted protocol risk in Phase 3, with the delivery state and the protocol date's firmness grade. Where account abstraction provides signature agility (EIP-8141-style validation logic, scheduled for inclusion in Hegotá with no activation date set and no post-quantum scheme specified in the EIP itself; Algorand's native Falcon-1024 accounts and Falcon authorizer today), adding PQC verification alongside classical is the closest on-chain analogue to the hybrid default and is piloted on testnets as it matures.

Algorithm Weighting for an All-ECC Estate

The Universal's algorithm-specific vulnerability weighting (Activity 3.1) applies in Phase 3: quantum attack cost scales with key size, not classical strength, so 256-bit elliptic curves are the first targets. The 2026 estimate sequence in the opening moved the 256-bit-curve figures down while the RSA figures did not. Digital assets are the extreme case of this weighting, for two compounding reasons. First, the asset class runs almost entirely on elliptic curves at the 256-bit scale (secp256k1 and Ed25519; BLS12-381, whose scalar field is 255 bits over a 381-bit base field) with no RSA legacy to dilute the exposure, and the exceptions this extension names (QRL's XMSS, Algorand's Falcon-1024 accounts, Solana's Falcon implementations) are the migrated or migrating minority.

Second, for every exposed public key on-chain (Challenge 1), the harvest step needs no collector. The key material and the value it controls are published on an immutable public ledger. The attacker needs no interception, no breach, and no waiting. 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 state (Challenge 1), and value at risk for every digital asset CBOM entry so that ranking reads recorded values rather than a judgment re-debated per holding. The IonQ estimate is specific to secp256k1. An Ed25519 or BLS12-381 entry has no curve-specific figure of its own. The absence of a figure is not evidence of lower exposure. The entry is scored on its data, its exposure state and its trust role like any other.

The Identity Stack in Track B

The Universal brings the identity stack explicitly into Track B scope. In digital assets that stack 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, and withdrawal approval workflows rely on device-bound credentials.

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 for Firmware and Release Signing

The Universal makes stateful hash-based signatures (LMS and XMSS, NIST SP 800-208) the component of Track B that deploys now (Two-Track Migration Model), 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 designated by CNSA 2.0 for software and firmware signing. 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.

"Deploy now" carries SP 800-208's own conditions, in section 8 of that publication: key and signature generation inside a hardware module with at least Level 3 physical security, no export of the private key in any form, and signing state managed inside the module so that backup, replication and failover designs cannot reuse a state. A signing service that does not meet section 8 is not a conforming deployment, and the verifiers must accept the parameter set chosen.

The action: move firmware and release signing pipelines to SP 800-208 signatures now, dual-signed with classical during transition, operated from HSM-backed signing infrastructure whose module certificate and entropy validation are recorded in the Phase 6 register, and add hardware wallet PQC verification capability to the Phase 7 vendor questions for wallet providers, second agility question first.

Securing the CBOM and Program Artifacts

The Universal's Activity 2.5 treats the CBOM and migration program artifacts as 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.

The default answer to each of them is the Universal's rule: attest, do not send. The attestation provider receives a signed commitment to the snapshot (a hash and its signing record), a coverage statement that gives its denominator and discovery method (Activity 1.2), and the predicate it needs ("every custodial address in the denominator is hash-protected or listed on the exposure register with a rotation date"; "no custody API

endpoint negotiated classical-only key establishment during the observation window"), in place of the address-to-value map.

Where a supervisor's examination powers require the record itself, it is a point-in-time extract scoped to the inquiry, delivered through a controlled channel, never standing access to the queryable inventory. Apply the remaining provisions of Activity 2.5 without exception: the CBOM repository is monitored with the same severity as the key management systems it describes, it is marked at the organization's highest handling class at generation, and access to it appears on the SOC's high-sensitivity exfiltration watch list.

Verification, Decommissioning, and Closure On-Chain

The Universal's Migration Verification & Program Closure section defines what "done" means, and digital assets gives it a twist in both directions. Verification is partly public. On-chain migration is independently observable: anyone can confirm that funds moved to quantum-resistant address types. Incomplete migration is equally visible to attackers. Custodial-side verification follows the Universal standard: observed algorithm negotiation on API and platform connections, negative testing once policy requires refusing classical-only peers, and a rehearsal record showing the custody stack's algorithm changed by configuration and rolled back.

Decommissioning is harder: an exposed public key cannot be removed from chain history. 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 reads three things. First, the Universal's four verification dispositions for every Tier-1 and Tier-2 service (migrated; migrated with agility debt and a funded closure date; enclosed or compensated under an accepted exception; retired), where an on-chain holding whose protocol has not activated a post-quantum path closes as enclosed or compensated under an accepted exception, with the address-rotation policy and the exposure register as the compensation.

Second, the closure proof: a rehearsed second algorithm change on at least one Tier-1 system per track, inside the agility window, minuted, with the segment timings in the evidence dossier; in this sector the Track B proof runs on the custody signing stack or the release-signing pipeline, because no on-chain key can be rehearsed. Third, the agility-debt register at zero unaccepted debt, where every remaining entry has a funded treatment with a date or a SteerCo-signed exception; protocol dependencies (a chain with no activated proposal, a precompile the deployer cannot change, an immutable contract) are recorded as SteerCo-signed exceptions carrying the protocol date and its firmness grade.

They are re-reviewed at the cadence the exception states rather than declared resolved. Closure hands protocol monitoring and governance participation to a standing function, because protocol-level PQC timelines (BIP-360 and BIP-361 activation, EIP-8141 and the Ethereum post-quantum roadmap, client PQC rollouts) will run for years after custodial migration completes.

The Agility Criterion and Rehearsal in Digital Assets

The Universal's agility criterion (Activity 4.6) asks four things of a migrated system: the negotiated outcome observed; classical-only refused and tested where policy requires it; the algorithm changeable by configuration; and a rehearsal in staging with the rollback exercised. In digital assets the four conditions apply differently on each side of the control boundary defined throughout this extension. On the custody signing stack, the exchange and custody APIs, node and validator management access, and firmware and release signing, all four can be met and are expected.

On an on-chain key, the third and fourth fail by construction: the protocol sets the algorithm, so the only algorithm change available is to move the asset to a new output type, account type or authorizer, which is a migration and not a configuration change. Where the protocol offers one already, that move is available now and is scheduled like any other migration. Where it does not, the entry waits on the protocol. This extension states the sector's agility objective in those terms.

An organization is crypto-agile when it can change the algorithm on its own custody stack, its own APIs and its own signing services on a planned date, and can name, per chain, the protocol change its on-chain keys wait on, the firmness grade of that change's date, and the address-rotation policy it applies in the meantime. Every wave includes an algorithm-change rehearsal on at least one system in the wave, chosen from the layer the organization controls: a parameter-set change (ML-KEM-768 to ML-KEM-1024) on an exchange or custody API endpoint; a hybrid-to-composite switch on the node-software or wallet-firmware release-signing pipeline; a key ceremony that generates a PQC-authorized signing key on the custody stack and retires it, which is the custody rehearsal.

A quarterly failover to the backup HSM partition exercises state management, failover and the SP 800-208 state design. It changes no algorithm, and it is recorded and reported as a failover exercise whose timings do not feed the rehearsed time-to-change KPI. Where a protocol already offers signature agility (a native rekey, an account-abstraction authorizer on a testnet), the rehearsal is an authorizer change on a test account, timed the same way.

Each rehearsal is timed across assessment, decision, change and verification, with the rollback exercised, scheduled outside settlement and reporting freezes, and its timings feed the rehearsed time-to-change KPI (KPI supplement). A rehearsal that cannot be scheduled because the change requires a protocol activation, a wallet-vendor release or

a hardware wallet replacement has found agility debt before production did. The entry goes to the Phase 3 register with its treatment.

Evidence Grades and the Coverage Denominator in Digital Assets

Every discovery finding is graded in the Universal's five tiers (Activity 1.2): E1, runtime observed; E2, binary confirmed; E3, inventory declared; E4, vendor attested; E5, inferred. In digital assets the distribution is unusual in one respect: the ledger is the production record, so the observed exposure state of every address, the admin roles on every contract and the signature scheme on every validator key are observed facts and grade E1.

Key control and migratability are not on the ledger and take the grade of the record or the assessment that states them, which is why Challenge 1 keeps the three claims apart. The custody stack grades the way any enterprise estate does: E1 from observed negotiation on API and platform connections, E3 from the HSM, KMS and multi-party signing exports, E4 from custody and wallet vendors' questionnaire answers, E5 for any upgrade mechanism or precompile dependency inferred from documentation rather than read from deployed bytecode.

Protocol roadmaps are E4 at best, from the foundation or client team that publishes them. The grade attaches to a claim, not to the row, and travels with the finding into the CBOM and into Phase 3, where an E5 entry scored Critical is a finding to verify before it is a finding to fund. Coverage is measured against a denominator enumerated before any chain scan runs: every address, account, contract and validator the organization controls or depends on, listed from the treasury records, the custody system of record, the portfolio and the staking records, never from what a scan found.

A scan that finds an address the records did not list is a denominator change reported with its cause. An address the organization did not know it controlled is an address whose exposure state nobody was managing, and it is escalated the day it is found. Asset classes the method cannot observe are named as unobserved with coverage recorded as unknown. One is holdings at a third-party custodian whose address set the custodian does not disclose.

Another is the exposure state behind an omnibus address the organization does not control. The accepted-gaps register, signed at gate G1 → G2 by the Discovery lead, the CISO and the SteerCo, records that scope with the reason and the closure date, and the same denominator is the one the on-chain quantum exposure KPI, the proof-of-reserves attestation and the Inventory Completeness KRI (Universal, GRC Implementation) all read.

Vendor Dates and Questions in Digital Assets

Every vendor and protocol date in this extension's tables and in the vendor scorecard is graded with one of the Universal's four firmness grades (Activity 7.5): committed (contractual, with remedies), forecast (a planning date stated in writing), announced (a public roadmap statement) or unknown. Phase 3 Dimension 3 scores the grade, not the calendar date. A protocol's date is never committed: no chain offers remedies, so a foundation roadmap grades announced at best, a proposal without an activation date grades unknown, and the Phase 4 timeline map carries each date at that grade.

The questionnaire opens with the two agility questions and the firmness question (Activity 7.2). For a custody platform, a multi-party signing provider or a node-software vendor, the first agility question establishes whether the signing stack changes algorithms by configuration or only with a release. For a hardware wallet vendor, the second question establishes whether the firmware verification key burned into devices already in drawers can follow an algorithm change at all.

A vendor whose answer is no has identified the sector's largest non-updatable verifier population. The four certificate-authority questions have a narrow scope in this sector: the public CAs behind exchange and custody TLS and the code-signing certificates on node and wallet releases. The non-standardized-algorithm rule and its one-afternoon test (Activity 7.3) apply to every wallet, custody product and chain marketed as quantum-safe on a proprietary or pre-standard scheme: a public specification with test vectors, published cryptanalysis, a standards-body track and a validated implementation. A product that fails the first two is excluded, and a Falcon deployment ahead of FIPS 206 passes the test and records the pre-standard dependency.

The provider-roadmap reading rule (Activity 7.7) applies to every cloud KMS and custody-as-a-service provider: the current negotiated state per service and the dated targets per service, graded, with the carve-outs read before any provider-side component is marked migrated. The Phase 7 adaptations place the whole set inside the vendor classification, with the protocol itself treated as a counterparty under Activity 7.6.

PHASE-BY-PHASE FRAMEWORK ADAPTATIONS FOR DIGITAL ASSETS

Phase 0 – Executive Mandate & Business Case

- **Dual-outcome charter:** The charter states both outcomes (Universal, Phase 0): quantum-safety readiness against the dated obligations that reach the organization (for an EU crypto-asset service provider, MiCA authorization with DORA's cryptographic-controls policy; elsewhere, the custody rules, client due diligence and insurer questions that name a date), and crypto-agility as the standing capability the migration builds. The charter names the on-chain estate as the population whose signature algorithm the organization does not set, so that the board reads its delivery state from the first report.
- **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.
- **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 the 1.7 million or more BTC in dormant exposed P2PK outputs (Google Quantum AI, March 2026; dormant, with owner and key-control status unknown) on exchanges would constitute a market event independent of any direct loss to the organization.
- **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.
- **Governance adaptation:** Name the Crypto-Agility workstream owner in the function that controls the custody stack, the APIs and the release-signing pipelines, with a budget line from Year 1 and the agility-debt register as scope, and name the

Cryptographic Record owner beside it (Activity 0.3). The SteerCo has a protocol-governance seat, held by whoever tracks the BIP, EIP, SIMD and ZIP processes for the portfolio, because the program's largest dependency reports through it and the refusal decision for a chain (Phase 7 adaptation) is taken there.

Phase 1 – Discovery & Inventory

Digital Asset-Specific Inventory Tracks

- **On-chain public key exposure, in three records:** For every chain in the portfolio, record every address, account and validator the organization controls under the three records of Challenge 1: the observed exposure state (no exposure observed in the assessed sources; exposed by format; exposed by history); the reported key-control status (controlled, or dormant with owner and key-control status unknown); and the assessed migratability under the protocol as it stands.

Record the value at risk in asset units beside them. Only the first is read from the ledger and grades E1. The second takes the grade of whoever reports it, and the third is an assessment recorded with its basis. For most account models there is no re-key without moving the asset. Where the protocol offers a native rekey or an account-abstraction authorizer, record it as the path.

- **Smart contract cryptographic dependencies:** Map all smart contracts the organization interacts with (DeFi protocols, stablecoins, bridges, oracles) and identify their admin key exposure (E1, from the role assignments on-chain), precompile dependencies, upgrade mechanisms (E2 where read from deployed bytecode, E5 where inferred from documentation), and, for every rollup and bridge, the proof system and the verifier implementation it depends on (Challenge 7).
- **Custodial infrastructure:** Inventory HSMs, key management systems, multi-party and threshold signing stacks, signing infrastructure, API authentication, and TLS configurations across all custodial platforms and exchange integrations, into the four-field register of Phase 6 (visible platform, firmware family, manufacturer of origin, certificate reference) with the entropy references; observed negotiation on API and platform connections grades E1, the module exports E3, vendor answers E4.
- **Validator/staking infrastructure:** For PoS chains, inventory validator key management, BLS signature implementations, and slashing protection mechanisms. The validator's signature scheme is an on-chain fact (E1) and the key-management platform behind it a custody entry.
- **Layer-2 networks and bridge dependencies:** Map Lightning Network channel exposure, cross-chain bridge cryptographic dependencies, rollup proof systems with their verifier lineage, and state channel implementations; "layer-2" is the protocols' own term for these networks and is not one of the framework's three numbered layer systems.

- **The denominator, before any scan:** Enumerate every address, account, contract and validator the organization controls or depends on from the treasury records, the custody system of record, the portfolio and the staking records before a chain scan runs, and measure coverage against that list. An address a scan finds that the records did not list is reported as a denominator change with its cause, and holdings at a third-party custodian whose address set is not disclosed are named as unobserved. The accepted-gaps register records the unreached scope and is signed at gate G1 → G2 (alignment section).

Phase 2 – CBOM & Documentation

Build the digital asset CBOM in three control classes: (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 class's PQC transition, with the firmness grade of every date.

Within the Universal's Minimum Viable CBOM model, the custody stack is CBOM Layer 2 platform cryptography and is covered first; on-chain and contract dependencies are CBOM Layer 3 application cryptography read from the ledger; wallet firmware and vendor signing stacks are CBOM Layer 4. Every entry follows the Universal's minimum record (Activity 2.1) with the sector's additions: the chain and network; the address, account or contract identifier; the curve and signature scheme; the observed exposure state, the reported key-control status and the assessed migratability (Challenge 1); the value at risk in asset units with a dated price assumption; the delivery state; and the protocol dependency that unblocks it, with its firmness grade.

Organizations carrying the CBOM in the Applied Quantum CBOM Profile (v1.0-RC or later) record the same facts as Profile properties. The Profile is informative carriage and never required, and the record stands without it.

Phase 3 – Risk Scoring & Prioritization

Adapted Risk Scoring Model

The Universal's four dimensions (Activity 3.1) stand: Dimension 1, data sensitivity and exposure (HNDL); Dimension 2, trust infrastructure criticality (TNFL); Dimension 3, migration feasibility; Dimension 4, regulatory and compliance pressure. This extension adds no dimension. The sector's factors are read inside the Universal's dimensions and scored with the Universal's arithmetic (Activity 3.2): Low = 1, Medium = 2, High = 3, Critical = 4; a dimension scores the highest of its factors; a dimension that does not apply to an entry is excluded with the weights renormalized; an unknown value is left unscored, listed and resolved before the entry is tiered.

- **Dimension 1 for on-chain keys:** A signing key that protects no confidentiality has no HNDL dimension. It is excluded and the composite is taken over the other three at the renormalized weights (TNFL 38.46 percent, regulatory pressure 38.46 percent, feasibility 23.08 percent), in which TNFL and regulatory pressure tie. Privacy-chain holdings and the off-chain stores (custody records, key shards, KYC archives) keep Dimension 1, with the confidentiality horizon set by the retention and privacy obligations that apply.
- **Observed exposure state (a factor inside Dimension 2):** Exposed on-chain, by format or by history = Critical (the harvest step is complete); no exposure observed in the assessed sources and never spent from = Medium (exposed at the moment of spending, the on-spend window). An exposed holding that is also dormant with key control unknown scores Critical on the same factor, read for the systemic scenario of Challenge 4 rather than for the organization's own remediation. Reported key-control status and assessed migratability are recorded beside the score and do not move it.
- **Value and control concentration (the Universal's scope-of-trust factor, read for the sector):** An admin, minter, pauser or upgrade key over a stablecoin, bridge or tokenized-asset contract, or a treasury key = Critical; a hot-wallet signing key or a validator key = High; a single customer address = Medium.
- **Verifier updatability (the Universal's Dimension 2 factor, read for the sector):** The factor scores the implementation that performs the verification, and nothing else. The verifier of an on-chain signature is the network's consensus rules, changeable only by protocol change = Critical, where those rules verify no post-quantum scheme the holding can move to; a hardware wallet with a burned-in firmware verification key = Critical; an EVM precompile a contract depends on = Critical; a custody stack whose verifiers the organization manages = Low.

A chain whose consensus rules already verify a post-quantum scheme, as Algorand's do for its Falcon accounts, is not scored as a physically non-updatable verifier. The constraint there is the organization's own migration, and the entry records the delivery state available. Enrolled customer credentials are read the other way round. For a WebAuthn assertion the relying party is the verifier. Its verification implementation is server-side and updatable, so enrolled passkeys score Medium or Low on this factor. The customer's authenticator holds the private key and signs.

What is hard is the signer side: re-enrolling every customer's authenticator on a new algorithm. Record signer-side migration difficulty and credential re-enrollment as a separate constraint against the entry, recorded in its delivery state, and score this factor on the verification implementation. Verifier updatability is the strongest single indicator of agility debt in the estate.

- **Control posture (the Universal's Dimension 3 factor):** Custody stack, APIs, release signing = Easy; a contract the organization can upgrade = Medium; protocol-governed = Hard, with the protocol date's firmness grade scored, not the date.

- **Weighting:** The Universal's default weights (HNDL 0.35, TNFL 0.25, regulatory 0.25, feasibility 0.15) stand for the custody estate; for on-chain entries the exclusion of Dimension 1 renormalizes them. The SteerCo ratifies the dimensions, the weights and the appeals rule before the first scoring run (Activity 0.3).

Delivery state and the agility-debt register. Every scored entry records a delivery state (available, dependent, blocked, unknown; Activity 3.2). An on-chain Track B entry is available where the protocol capability and the practical signer and verifier tooling both exist and the move is the organization's own to make, dependent where an identified external delivery is still required, and blocked where no feasible approved path exists.

Chain-wide consensus risk is recorded on its own line and does not convert an actionable migration into a dependency. The entry keeps the tier the ordered test gives it and is never demoted for the block. It is shown with the dependency that unblocks it (the output type, account type, precompile or fork) and that dependency's firmness grade, and it appears on the roadmap against its unblocking date (Phase 4 adaptation). The agility-debt register lists every Tier-1 and Tier-2 entry scored Hard on control posture or Critical on verifier updatability, with the reason: every on-chain key (the algorithm is set by the protocol), every hardware wallet with a burned-in verifier, every contract whose code is immutable or whose upgrade authority the organization does not hold, and every EVM precompile dependency.

The register is derived from the scores already recorded, adds no dimension, feeds the Crypto-Agility workstream and the Phase 4 roadmap, and reaches zero unaccepted debt before closure, with protocol dependencies as SteerCo-signed exceptions (alignment section). How many distinct verifier lineages, firmware families or key-generation designs execute beneath the portfolio's rollups, custodians and vendors is a Cryptographic Concentration Framework question (CCF layer 2, implementation lineage; CCF layer 4, custody), cross-referenced in the Quantum Readiness Assessment and not computed here.

Digital Asset Priority Tiers

Priority	System Category	Rationale	Typical Delivery State
Tier 1	Every on-chain key the organization controls or depends on, in every exposure state: exposed keys (P2PK, Taproot key paths, spent-from or reused addresses, EOAs that have sent),	Placed by the ordered test of Activity 3.2: Dimension 2 Critical on any factor (verifier updatability, because an on-chain signature's verifier is the chain's consensus	Available for the custody trust anchors, the identity stack, the internet-facing endpoints, and any chain that already offers a post-quantum authorizer or output type the

Priority	System Category	Rationale	Typical Delivery State
	hash-protected never-spent-from custodial addresses, treasury keys, hot-wallet signing keys, validator keys, smart contract admin, minter, pauser, upgrade and bridge keys, the oracle and bridge signing keys that contracts verify, and the proof systems and polynomial commitments behind rollups, bridges and privacy pools; Lightning channel keys and rollup and bridge dependencies; privacy-chain holdings; the host chains of the tokenized assets in the portfolio; the custody estate's trust anchors (HSM and KMS wrapping roots, multi-party signing stacks and the approval trust anchors relied on across the custody estate); customer passkeys and device-bound credentials enrolled on devices the organization cannot update, and the identity provider's signing key; every	rules, which no campaign reaches; exposure state, where the harvest step is complete; scope of trust, for a key that controls a contract's roles or a treasury, for a trust anchor relied on across the custody estate, and for an identity provider's signing key the whole estate authenticates against); or Dimension 1 Critical with accessibility High or Critical (an internet-facing endpoint; a privacy-chain holding, whose transaction data is recorded on a public ledger with a confidentiality horizon over 15 years); or Dimension 4 Critical (a mandatory deadline within 2 years, which no instrument in this map has at this edition). Challenge 7 classifies on-setup exposure at the highest severity and Challenge 8 states retroactive privacy loss as irreversible; the test places both	holding can move to; dependent where the chain has a dated proposal or the move waits on an identified external delivery; blocked where no feasible approved path exists. A blocked entry keeps this tier and names its bridging pattern on the record (below). Enrolled customer credentials are not placed here by verifier updatability, whose subject is the relying party's verification implementation; where they sit in this tier they sit there on the risk their own dimensions give them, with the re-enrollment campaign recorded as their constraint

Priority	System Category	Rationale	Typical Delivery State
	internet-facing exchange, custody and node endpoint (API TLS, request-signing keys, public RPC)	here.	
Tier 2	Off-chain stores with a confidentiality horizon over 10 years on internal interfaces: custody records, key shards and their backups held in-house, KYC and transaction-monitoring archives; internal custody platform communications carrying that data; key establishment between the parties of a multi-party signing stack inside the organization's own network; a custody, wallet or signing-stack arrangement under a client or partner contract that requires PQC; any entry under a mandatory deadline within five years should a supervisor's instrument reach enforcement tier 2 or 3	Dimension 1 Critical or High with internal accessibility (a store whose horizon exceeds 15 years meets the first condition only when it is internet-facing or partner-facing; key shards held at a third party are partner-facing and belong in Tier 1), unless the entry is air-gapped; or Dimension 2 High (a signing key inside the custody stack whose verifiers the organization manages and whose signatures several applications rely on, a shared intermediate, verifiers updatable by campaign); or Dimension 4 High (a mandatory deadline within 5 years, or a contract that requires PQC).	Available: the organization controls both ends of every entry here; where a stack changes algorithms only with a vendor release, that release carries a firmness grade on the record

Priority	System Category	Rationale	Typical Delivery State
Tier 3	Entries whose highest applicable dimension is Medium: the internal management plane (SSH to nodes and validators, internal RPC, monitoring and telemetry) carrying data with a horizon of over 5 to 10 years; single-application signing keys inside the custody stack verified by centrally managed trust stores within one system; short-lived session tokens, whose signing keys are their own entries above; entries under a general regulatory expectation only	Any applicable risk dimension (1, 2 or 4) Medium or above, and none High or Critical. Plan now; execute in the roadmap's later waves.	Available, dependent or blocked as the record states; the delivery state moves the roadmap date and never the tier
Tier 4	Entries whose every applicable risk dimension is Low: an internal or air-gapped entry carrying data with a horizon of 5 years or under, with no signature role beyond one session or process and no regulatory expectation attached, such as an internal test environment holding no production key	Every applicable risk dimension Low. Monitor; compensating controls; migrate when feasible. A blocked migration does not place an entry here: layer-2 networks, privacy-chain exposure, proof-system dependencies and tokenized-asset host-chain risk are tiered on their risk above, take the	Blocked entries are shown in the tier the ordered test gives them, not in this one

Priority	System Category	Rationale	Typical Delivery State
	material or a public market-data feed consumed without a signature dependence. Few entries in a digital asset estate meet the condition	delivery state blocked or dependent, and run under their bridging pattern	

Bridging patterns for blocked Tier-1 entries. No overlay of Activity 7.4 reaches a consensus rule, so an on-chain entry blocked on a protocol change names Activity 7.4's documented residual-risk acceptance on its record, with the protocol activation as the re-evaluation trigger, the exposure register and, where the chain's address model supports one, the address-rotation policy as the compensating controls, and the value held on the chain as the variable the refusal decision of Phase 7 can reduce. A hash-protected never-spent-from output carries the same acceptance with the on-spend window as the exposure it records.

Where a chain already offers a post-quantum authorizer or output type, the entry is available: the migration is the organization's own to schedule, and it is neither dependent nor blocked. A contract whose code is immutable or whose upgrade authority is held by another party, an EVM precompile dependency, a proof system with a trusted setup and a Lightning channel are blocked on the same terms, with the contract's upgrade path, the precompile proposal (EIP-8355, grade unknown), the proof system's replacement or the channel's closure and re-opening on a migrated output as the trigger.

A timelock on its own does not put a contract here: it delays an authorized operation. The record shows that delay beside the upgrade authority rather than in place of it. A privacy-chain holding has no bridge: the exposure is recorded under Challenge 8, the retroactive loss is accepted or the holding is exited, and no future protocol change is recorded as remedying transactions already on the ledger. A hardware wallet with a burned-in verification key is blocked until the vendor's replacement or firmware line ships, and the wallet population is listed with that date and its firmness grade.

Phase 4 – Roadmap & Governance

Protocol-Specific Timeline Map

The roadmap incorporates protocol timelines the organization does not control. Every date below is graded for firmness (Activity 7.5: committed, forecast, announced,

unknown). A protocol date is never committed, and Phase 3 Dimension 3 scores the grade. An on-chain entry that waits on one of these dates keeps its tier, takes the delivery state dependent or blocked, and appears on the roadmap against the date with its grade. Each protocol is a counterparty under Activity 7.6 (Phase 7 adaptation), and the map is re-checked at each release, because every line below moved between the June and September 2026 editions:

- **Bitcoin:** BIP-360 (P2MR, a script-path-only output type that removes Taproot's key path and adds no post-quantum signature scheme; BIP number assigned December 18, 2024, renamed P2MR February 10, 2026, Draft) and BIP-361 (legacy signature sunset; assigned February 11, 2026, Draft, dependent on a post-quantum output type no assigned BIP yet defines). No activation timeline as of September 2026. Grade: unknown; delivery state of every Bitcoin on-chain entry: blocked, with address rotation to never-spent hash-protected outputs as the compensating control. Monitor Bitcoin Core development and miner signaling.
- **Ethereum:** On September 7, 2026 the Ethereum Foundation Protocol cluster published a cluster-wide commitment that Ethereum layer 1 will be quantum-resistant across execution, consensus and data by December 2029, treated as non-negotiable at least until January 2027, when quantum progress is reassessed with outside experts. The post states that layer 1 should plan for Q-day as early as 2030 and calls that a deliberately aggressive assumption against most credible estimates.

Its milestones: the post-quantum public-key registry at I*; a minimum-viable post-quantum milestone at J*, comprising the post-quantum heartbeat on consensus, leanDA sampling on data and leanSPHINCS transactions on execution, described as a temporary safeguard that keeps the chain operating through Q-day with reduced guarantees not yet defined; and full readiness at L*, five hardforks after Glamsterdam, requiring a 7.2-month average cadence the Foundation itself calls aggressive.

This supersedes the Post-Quantum team's June 27, 2026 assessment that layer-1 upgrades could complete by 2029. Supporting proposals, read from EIP-8081: EIP-8141 (Frame Transaction, signature agility) scheduled for inclusion in Hegotá, Draft, with no activation epoch or date on any network and no post-quantum scheme specified in it; EIP-8355 (precompiles for ML-DSA verification) at Proposed for Inclusion and not scheduled; EIP-8298 and EIP-8151 as the account path for retiring secp256k1 as a master key and EIP-8365 for withdrawal credentials, none of the three scheduled. pq.ethereum.org weekly interoperability devnets with more than ten client teams (launched March 25, 2026).

Grade: announced. A cluster-wide commitment with a stated reassessment date is firmer than the June assessment in every respect except the one the vocabulary measures, which is contractual remedies, and no chain offers those. The Foundation's own maturity pipeline runs research, EIP, prototype, devnet, PFI, CFI, SFI and mainnet, and it says of the last three signals that they "do not substitute for implementation

evidence." Delivery state of Ethereum on-chain entries: dependent, on EIP-8355 for contract-verified post-quantum authorization at workable cost and on the registry and minimum-viable milestones for protocol-native support; moving a holding to a fresh account that has never sent reduces at-rest exposure and is available now, carrying the on-spend exposure recorded against it.

- **Solana:** The Anza and Firedancer validator client teams independently selected Falcon and published initial implementations. The Solana Foundation's phased plan (April 27, 2026) states that no protocol change is required today and names no date. Grade: announced, no date; delivery state: blocked until a SIMD carries an activation. Monitor SIMD proposals for the PQC integration timeline.
- **Zcash:** ZIP 2005, Ironwood Quantum Recoverability, activated on mainnet with NU6.3 on July 28, 2026 (ZIP 258; the June 2026 edition recorded it as the May 7, 2026 forecast under the name Orchard quantum recoverability). The ZIP states that it does not by itself make the protocol quantum-secure, and funds in the Sprout, Sapling and Orchard pools migrate to the Ironwood pool to gain recoverability (Zcash moved to Orchard/Halo 2 in 2022, removing the trusted-setup dependency; Orchard remains quantum-vulnerable on its curve assumptions).

Full post-quantum status was targeted at the May 7, 2026 announcement within 12 to 18 months through Project Tachyon, a 2027 target. Grade: the Ironwood activation is a ledger fact and the Tachyon target is announced; delivery state: dependent, with the migration of the organization's own shielded holdings to the Ironwood pool available now.

- **NIST IR 8547:** Proposes deprecating quantum-vulnerable public-key algorithms at 112-bit strength after 2030 and disallowing all of them after 2035; still a draft at this edition. Sets the outer boundary for any chain that has not migrated, and it is the reference most other instruments are built against (Universal, Regulatory Timeline Context).

These protocol dependencies are visualized on one timeline map with their grades and reviewed quarterly by the protocol-governance seat. Where a protocol date slips or a proposal is withdrawn, the roadmap adapts through the Re-Baseline Protocol (Activity 4.8): a chain whose activation moves beyond the horizon the roadmap assumed opens a re-baseline review at the next SteerCo, minuted to the evidence dossier, with the authority that owns the date moving it. Internal preparation (Phases 0 to 3) and the migration of everything the organization controls proceed regardless of protocol readiness.

Gates and Recorded States

Every gate record from G5 → G6 onward, and every wave-exit record, shows two results as separate fields (Universal Activities 4.6 and 5.4): the protection result (which functions and boundaries are verified, which remain exposed) and the agility result (which change was rehearsed, through which mechanism, in what elapsed time, with

which constraints). A custody API that passes on protection and whose gateway can change its algorithm by configuration exits as migrated. A custody signing stack that passes on protection behind a vendor release exits as migrated with agility debt, with the entry and its closure date in the Phase 3 register. An on-chain holding is never shown as migrated on the strength of the custody stack around it, and its own record shows the protection result with the agility result recorded against the protocol.

Observing that funds moved establishes movement and not protection. Funds can move from one vulnerable authorization scheme to another, so the protection result names the destination's authorization scheme, the active authorizer, the signer and tooling support behind it, the verification actually tested, and any recovery or admin path. A move to a hash-protected classical output is recorded as exposure reduction with residual on-spend risk.

Post-quantum protection is credited only where the required post-quantum authorization is enforced on the destination. The Coverage and Agility KPIs read the two results separately.

Phase 5 – Pilots & Migration

- **Custodial infrastructure hybrid TLS:** Enable hybrid ML-KEM + X25519 on exchange APIs and custodial platform endpoints. Lowest-risk starting point.
- **Address hygiene enforcement:** Eliminate address reuse across all custodial UTXO management. Where a holding's threat model is the at-rest attacker over a multi-year holding horizon and the holding does not depend on a Taproot script path, move funds from Taproot (P2TR) addresses to hash-protected SegWit addresses to reduce at-rest exposure. The move is a decision per holding under the written address-rotation policy, with its costs recorded, and it is not applied to every holder.

Before the move, map the holding's specific spending conditions and whether the destination can express them: multisignature and some timelock policies can be written in P2WSH, so only a Tapscript feature the destination genuinely cannot carry is a loss, and it is recorded as a documented cost rather than assumed from the output type. The address-rotation policy carries, per chain and per holding: the current account or output type; the public-key exposure it creates; any native rekey or authorizer the protocol offers; wallet support; transaction cost; and the residual risk left after the move, including the discipline that keeps the new output never spent from.

It offers hash-protected rotation only where the chain's address model and the holding's spending requirements both support it. A classical hash-protected destination reduces exposure and does not make the holding post-quantum, and the record says so.

- **PQC signature testing on test networks:** A public testnet does not simply mirror mainnet. Public testnets routinely activate future rules first: Hoodi ran Pectra ahead of its mainnet activation in 2025. The constraint is that the particular network used

must implement the proposed verification rules. Record, per test: the network; the client and version; the consensus feature flags or patches in force; and the activation state at the time of the test.

Native post-quantum transaction signing runs on a network carrying the proposed rules (Bitcoin regtest or a custom Signet with a post-quantum signature scheme enabled, an interoperability devnet of the kind pq.ethereum.org runs, a maintained devnet or a private cluster running a client team's implementation, or modified clients where no maintained network carries the rules) or on a signaling fork. Keep those tests separate from contract-level verification tests, which run on Ethereum Sepolia, Hoodi or the current equivalent and on Solana devnet, where post-quantum verification is implemented inside contract or authorizer logic under the rules already in force. Measure signature size impact on throughput, fees, and client compatibility on the network whose rules the measurement is about.

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

The Rehearsal per Wave and the Wave-Exit Criterion

Every wave includes an algorithm-change rehearsal in staging on at least one system in the wave (Activity 5.2), chosen from the layer the organization controls: a parameter-set change from ML-KEM-768 to ML-KEM-1024 on an exchange or custody API endpoint; a hybrid-to-composite switch on the node-software or wallet-firmware release-signing pipeline; a key ceremony that generates a PQC-authorized signing key on the custody stack and retires it, the custody rehearsal; on a chain with a native rekey or an account-abstraction authorizer, an authorizer change on a test account.

The quarterly failover to the backup HSM partition exercises state management, failover and the SP 800-208 state design. It changes no algorithm, and it is recorded and reported as a failover exercise whose timings do not feed the rehearsed time-to-change KPI. The rehearsal is timed across assessment, decision, change and verification, with the rollback exercised, scheduled outside settlement and reporting freezes, and the four elapsed times feed the rehearsed time-to-change KPI.

Every wave exit from Wave 1 onward applies the agility criterion (Activity 4.6): negotiated outcome observed; classical-only refused and tested where policy requires it; algorithm changeable by configuration; rehearsal run with the rollback exercised. A custody system that fails the last two conditions exits the wave as migrated with agility debt. An on-chain holding exits with its agility result recorded against the protocol and its protection result stated as the destination's authorization scheme, the active authorizer, the signer and tooling support, the verification tested and any recovery or admin path, rather than as movement observed on the ledger. The wave-exit record shows both results for every system in the wave.

Wave 3 (external, controlled) is where the organization applies the counterparty pattern to its exchange integrations and API consumers: published dual-stack windows on API versions, interoperability test events before enforcement, and the refusal decision recorded for the counterparty that will not move.

Phase 6 – Infrastructure & Performance

The HSM, KMS and Signing-Stack Register

The Universal's Activity 6.2 register is the Phase 6 instrument for the whole custody estate: HSMs, cloud KMS, and the multi-party and threshold signing stacks that hold key shares in software. It records, for each module or stack: the visible platform (the product as procured), the supplier's canonical firmware family (for a multi-party stack, the signing library and its version), the manufacturer of origin, and the FIPS 140-3 certificate reference where one exists.

Two products under two names can be one firmware family; a cloud KMS is recorded as a dependency boundary rather than as a manufacturer; a multi-party stack that wraps an HSM-held share records both. The four fields are recorded separately, and the boundary-verification rule of Activity 7.7 applies to the cloud rows. Key generation and entropy are recorded beside them: every module or stack that generates a long-lived signing key or a PQC key draws from an SP 800-90B validated source, with the ESV certificate reference (or the ENT designation on the module certificate) and the operating envelope recorded, and for a multi-party ceremony the generator of every participating party is recorded.

Custody key generation is where the sector's largest concentration of value meets its smallest population of generators. A "quantum" label on a randomness product is not a requirement of this framework or of any standard it cites. Organizations that keep the register in a Profile-conformant CBOM record the same facts as `custody:*` and `entropy:*` properties. The register stands without them. Whether two custody products share one firmware family or one signing library is a Cryptographic Concentration Framework question (CCF layer 4, custody; CCF layer 6, key generation), cross-referenced from the register.

Nothing in the register changes the algorithm the ledger verifies. The register describes how a secp256k1 or Ed25519 key is generated, held and used, and the on-chain entry for that key keeps its own delivery state.

- **HSM PQC readiness for custodial signing:** Record, per module, whether the custodial HSM supports PQC key generation and signing. Record whether that operation is inside the validated boundary of the certificate the register cites (alignment section). The answer to the first agility question sets the class. Plan firmware upgrades or hardware replacement where the operation is not covered. PQC on the custody HSM protects the wrapping, the approvals and the transport around the signing

operation. The signature the chain verifies stays the protocol's until the protocol changes.

- **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.
- **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

The Protocol as a Counterparty

The Universal's counterparty pattern (Activity 7.6) assumes a counterparty that can be negotiated with. A protocol cannot, and this extension reads each of the pattern's six elements for it. Readiness discovery is read from the ledger and the proposal record (the output types the chain accepts, the proposals merged, the devnets running), not from a questionnaire. Dual-stack windows are the protocol's own transition periods (a new output or account type coexisting with the legacy types), and the organization's window is the period during which it holds assets on both.

The deprecation protocol is the protocol's sunset proposal where one exists (BIP-361's phases), and the organization's own deprecation schedule for exposed address types. Interoperability test events are the testnets, signets and devnets (Phase 5). API versioning is the new output type, account type or authorizer the protocol introduces, which the organization migrates to by choice of address. The refusal decision is taken for the chain whose governance will not move: a documented risk acceptance with the address-rotation policy and the exposure register as compensating controls, a reduction of the value held on the chain, or exit, and it belongs to the business owner of the holding, made on the program's evidence, and goes in the risk register either way. Every protocol date is graded for firmness (Phase 4 adaptation).

Digital Asset Vendor Classification

The table groups the sector's counterparties and vendors by role. Entities a reader deals with regardless of choice (protocol foundations and client teams, standards bodies) are named as public facts; entities a reader selects among (exchanges, custodians, wallet vendors, audit firms, HSM and key-management vendors) are described by class, with the names the June 2026 edition listed in Tool and Vendor References. Alternative sourcing removes a dependency only if the alternative does not share it; whether two custody products, two wallets or two rollups run on one implementation lineage is a question for the Cryptographic Concentration Framework, and the vendor register records its result by cross-reference.

Vendor Category	Examples	Engagement Approach

Vendor Category	Examples	Engagement Approach
Protocol development teams and foundations	Bitcoin Core maintainers; the Ethereum Foundation and the client teams; Anza and Firedancer for Solana; the Zcash Foundation and the Zcash development organizations	Monitor BIP/EIP/SIMD/ZIP proposals. Participate in governance. Fund PQC development where appropriate. Treat as a counterparty under Activity 7.6; grade every date for firmness.
Custodial and exchange platforms	Custody providers, exchanges and custody-as-a-service platforms (Tool and Vendor References)	The two agility questions and the firmness question first. PQC readiness questionnaires. HSM and signing-stack upgrade timelines. Address reuse audit against the exposure register. The provider-roadmap reading rule for custody-as-a-service (Activity 7.7).
Wallet software and hardware providers	Hardware wallet vendors, software wallets and wallet SDKs (Tool and Vendor References)	The second agility question decides the class: can the firmware verification key in devices already in the field follow an algorithm change. Monitor PQC signature support. Hardware wallet PQC capability timelines, graded. SP 800-208 for firmware signing.
Multi-party and threshold signing providers	MPC and threshold signing platforms and libraries (Tool and Vendor References)	Register entry with the signing library and version. The two agility questions. Entropy references per party. Whether two providers share one signing library is a CCF question.
Smart contract audit firms and proof-system providers	Audit firms; rollup, bridge and proof-system providers	Include quantum vulnerability assessment in smart contract audits: admin key exposure,

Vendor Category	Examples	Engagement Approach
	(Tool and Vendor References)	precompile dependencies, upgrade paths. Ask which specification the verifier implements, whether the transcript binding of every prover-supplied value has been reviewed against it, and which other deployed verifiers share the lineage (Challenge 7).
HSM and key management vendors	HSM vendors and cloud KMS providers (Tool and Vendor References)	Same engagement as the Financial Services Extension's Phase 7: agility questions first, then PQC firmware, validation and certification timelines per firmware family, graded; the cloud KMS rows under the boundary-verification rule.

Questionnaire Order and the Acceptance Test

The vendor questionnaire of Activity 7.2 is asked of every custody, wallet, signing and node-software vendor in the Universal's order: the two agility questions first (can the algorithm be changed by configuration without recompilation, reinstallation or hardware replacement; can the verifiers and trust stores be updated in the field), then the firmness grade of every date, then the feature, GA-date, interoperability, performance, fallback and CBOM questions.

The Universal's procurement clause (Activity 7.3) warrants configuration-driven algorithm change, and the acceptance test turns the clause into evidence: before a custody platform, a signing stack or a wallet integration enters production, the organization's own team executes a rehearsed algorithm change on the product using the rehearsal pattern of Activity 5.2, with the elapsed times recorded and the rollback exercised. A product that passes its functional acceptance tests and fails the rehearsal has not met the clause.

The non-standardized-algorithm rule and its one-afternoon test (Activity 7.3) apply to every wallet, custody product and chain marketed as quantum-safe on a proprietary or pre-standard scheme (alignment section). The four certificate-authority questions go to the public CAs behind exchange and custody TLS and to the code-signing issuers for

node and wallet releases, and every cloud KMS and custody-as-a-service provider is asked for both halves of the roadmap disclosure (Activity 7.7).

DIGITAL ASSETS REGULATORY ALIGNMENT MAP

Digital asset regulation is fragmented across jurisdictions. No jurisdiction had, at this edition, mandated PQC migration for blockchain-native assets. Two instruments reach the organizations this extension addresses, and both are read through the Universal's mechanism: the deadline archetype each sets, the enforcement tier at which it binds, and the framework output that satisfies it. Supervisory expectations for digital-asset service providers are moving from advisory to expectations, and the verified instance is European: since July 1, 2026, the end of the transitional period under Article 143(3) of the Markets in Crypto-Assets Regulation (Regulation (EU) 2023/1114), every crypto-asset service provider operating in the EU either holds a MiCA authorization under Article 59 or provides the services under the Article 60 notification route open to entities already authorized under other EU financial-services law (credit institutions, central securities depositories, investment firms, electronic money institutions, UCITS management companies, alternative investment fund managers and market operators), which notify their competent authority at least 40 working days before starting.

An authorized provider is a financial entity under DORA (Regulation (EU) 2022/2554, Article 2(1)(f), as ESMA reads it). An Article 60 notifier is one already in its primary capacity under Article 2(1). The policy on encryption and cryptographic controls with its provision for updating or changing cryptographic technology as cryptanalysis develops (Commission Delegated Regulation (EU) 2024/1774, Article 6) binds it without a PQC date, which makes the crypto-agility obligation current rather than future.

Jurisdiction rows that repeat the Universal's roster (NIST IR 8547 and the national timelines) are not reproduced here. The roster is in the Universal's Regulatory Timeline Context and, kept current, on the Global PQC Migration Clock page, and the instruments that bind a given organization are recorded in its Regulatory Horizon Report (Universal, GRC Implementation).

The table is a dated snapshot as of September 2026. The enforcement tiers follow the Universal's definition of the tier by who enforces (tier 1, market access; tier 2, supervisory directive with a named enforcer; tier 3, binding government mandate with an audit trail; tier 4, authoritative guidance; tier 5, advisory); Phase 3 Dimension 4 reads the tier. Every date is re-checked against its instrument at each release, and readers verify status and applicability for their own organization before planning against a row.

Instrument	Requirement and dates	Status at this edition (enforcement tier)	Framework phases and digital-asset implication
MiCA, Regulation (EU) 2023/1114 (crypto-asset service provider regime; Title V)	Authorization under Article 59, or notification under Article 60 for entities already authorized under other EU financial-services law, required to provide crypto-asset services in the EU; the CASP regime applicable from December 30, 2024; transitional period for providers operating under national law ended on July 1, 2026 at the latest (Article 143(3)); ICT risk management for authorized providers governed by DORA	In force; transitional period closed (tier 3: binding EU regulation, with the authorization itself a market-access gate enforced by the national competent authorities)	Phase 0 and Phase 4: the authorization is the obligation the charter names for an EU provider; the date from which the DORA row binds.
DORA, Regulation (EU) 2022/2554, with the RTS on the ICT risk management framework, Commission Delegated Regulation (EU) 2024/1774 (Articles 6 and 7), as it reaches crypto-asset service	A policy on encryption and cryptographic controls, with provisions for updating or changing cryptographic technology on the basis of developments in cryptanalysis, and	In force (tier 3: binding EU regulation with supervisory examination and reporting obligations)	Phase 0, 4 and 7: the crypto-agility obligation is current; the procurement clause and its acceptance test, the rehearsal records, the custody register and the verification records are the DORA ICT risk evidence for

Instrument	Requirement and dates	Status at this edition (enforcement tier)	Framework phases and digital-asset implication
providers under Article 2(1)(f)	key-management rules; in application since January 17, 2025; binds a crypto-asset service provider from its MiCA authorization, and an Article 60 notifier in its primary capacity; no PQC date		a custodian or exchange.

Enforcement tiers the Universal does not assign are recorded here as this extension's reading: MiCA tier 3, DORA tier 3. Three rows the June 2026 edition included are not reproduced. The first is the US custody and securities regulators (an evolving expectation with no sector date; a proposed custody framework reported to reference NIST PQC algorithms is on the verify-first register and enters the map when verified against the instrument).

The second is the Asian supervisors' quantum readiness expectations for virtual asset service providers (no instrument with a date verified for this edition; the HKMA readiness index and the FINMA guidance are financial-sector instruments covered in the Financial Services Extension). The third is the BIS and FSB financial-stability work (advisory, tier 5, in the Financial Services Extension's map as BIS Papers No. 158). Regulated custodians, exchanges, and tokenized asset issuers fall under broader financial regulation as it evolves. The Regulatory Horizon Report records the instruments that bind each organization.

DIGITAL ASSETS MATURITY MODEL SUPPLEMENT

The levels, names and descriptions are the Universal's single 0 to 5 scale (Maturity Levels), used by the enterprise model and every per-phase table alike. The sector indicators are read beside them; from Level 2 upward each level describes the on-chain estate separately from the custody estate, because the two carry different delivery states.

Level	Universal Level	Digital Asset Indicator
0	Unaware: no organizational awareness of quantum cryptographic risk; no activities planned or underway	No sector indicator.
1	Aware: quantum risk acknowledged at leadership level; initial education conducted; no formal program	No assessment of on-chain public key exposure. No inventory of custodial HSM, KMS or signing-stack PQC readiness. No monitoring of protocol-level PQC proposals (BIPs, EIPs, SIMDs, ZIPs).
2	Initiated: formal program chartered; budget allocated; discovery underway; initial CBOM in development	Charter states both outcomes and names the on-chain estate as protocol-governed; Crypto-Agility and Cryptographic Record owners named; protocol-governance seat on the SteerCo. On-chain exposure quantified by chain, address type and exposure state, against a denominator enumerated from the treasury and

Level	Universal Level	Digital Asset Indicator
		custody records, with the accepted-gaps register signed. Custodial estate in the four-field register. Smart contract admin key exposure assessed. Protocol PQC timelines tracked with firmness grades. Initial QRA produced, with the on-chain delivery states stated on their own.
3	Progressing: CBOM operational; risk scoring complete; hybrid pilots in production; vendor engagement active; KPIs reported	Scoring model ratified with the sector factors; agility-debt register produced, with the on-chain population and the hardware-wallet population as their own lines. Protocol-specific timeline map maintained with grades and reviewed quarterly. Address hygiene enforced (no reuse, no unnecessary Taproot key-path exposure) under a written address-rotation policy. Custodial hybrid TLS pilots run; first algorithm-change rehearsal run on the custody stack (a key ceremony generating and retiring a PQC-authorized signing key) or on a custody API endpoint (a parameter-set change) and timed; the HSM-partition failover recorded as a failover exercise. Industry governance participation active. Custody and wallet vendor roadmap reviews quarterly, agility questions answered.

Level	Universal Level	Digital Asset Indicator
4	Advanced: Tier-1 systems migrated to hybrid/PQC; PKI modernized; crypto-agility demonstrated; vendor commitments secured	Hybrid key exchange on custodial APIs with the negotiated outcome observed. PQC signing tested on testnets, signets and devnets. Funds migrated from exposed addresses where the protocol permits, observed on the ledger, and the remainder recorded as dependent or blocked with the unblocking dependency and its grade. Validator keys on PQC-ready infrastructure where the chain supports it. Two results in every gate and wave-exit record. An algorithm change rehearsed on the custody stack and on the release-signing pipeline inside the agility window. Firmware and release signing on SP 800-208, dual-signed. Contractual crypto-agility with the acceptance test in every new custody, wallet and signing-stack arrangement.
5	Optimized: estate-wide PQC migration substantially complete; crypto-agility is organizational capability; continuous monitoring and posture management operational	All custodial infrastructure quantum-safe or hybrid. On-chain holdings on PQC-native address types wherever a protocol offers them, and every holding on a chain that does not offer them carries a SteerCo-signed exception with the protocol date, its grade and the address-rotation policy. Smart contract interactions limited to PQC-upgraded protocols or recorded as accepted

Level	Universal Level	Digital Asset Indicator
		exceptions. Standing rehearsal cadence on the custody stack, the APIs and the signing pipelines; the closure proof run per track. Agility-debt register at zero unaccepted debt: every remaining entry funded with a date or under a SteerCo-signed exception. Protocol monitoring and governance participation transferred to a standing function.

DIGITAL ASSETS KPI SUPPLEMENT

Board-Level KPIs (Quarterly)

- **On-chain quantum exposure:** Value held in addresses with exposed public keys / total custodial value, each figure against the enumerated denominator, with the exposed-and-unmigrable population reported on its own line. Target: converging toward zero through address migration where the protocol permits. Where the protocol does not permit it, the target is the written address-rotation policy.
- **Custodial infrastructure PQC readiness:** Percentage of custodial HSMs and signing systems with PQC capability / total custodial infrastructure.
- **Protocol PQC timeline alignment:** Number of chains in portfolio with activated PQC support / total chains held. Tracking metric for external dependency.
- **Smart contract admin key exposure:** Value controlled by smart contracts with quantum-vulnerable admin keys / total smart contract exposure.

Operational KPIs (Monthly)

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

Agility KPIs (CISO cascade, monthly; summarized to the board under the Agility KPI)

The four agility KPIs of the Universal (Metrics, KPIs & Reporting) are measured on the layer the organization controls, and the on-chain population whose algorithm the protocol sets is reported beside them, never inside them.

KPI	Digital asset measurement	Threshold
Configuration-driven share	Percentage of Tier-1 and	Target by year from the

KPI	Digital asset measurement	Threshold
	Tier-2 custody systems (the HSM, KMS and multi-party signing stacks, the exchange and custody APIs, node and validator management access, the release-signing pipelines) whose key-establishment and signature algorithms change by configuration, verified by rehearsal; on-chain keys and hardware wallets in the field are their own lines and never enter the numerator	roadmap's agility milestones; a year missed by more than 10 points triggers Crypto-Agility workstream review
Rehearsed time-to-change	Elapsed time across assessment, decision, change and verification on the most recent rehearsal, per track: on an exchange or custody API endpoint for Track A; on the custody signing stack (a key ceremony generating and retiring a PQC-authorized signing key; the quarterly HSM-partition failover is recorded as a failover exercise and its timings do not enter this KPI) or the release-signing pipeline for Track B (Activity 5.2), scheduled outside settlement and reporting freezes	Inside the agility window; a rehearsal whose change segment cannot run without a protocol activation, a wallet-vendor release or a hardware replacement has found agility debt on that system, recorded in the register rather than as a variance
Agility-debt burn-down	Entries closed on the Phase 3 register per quarter, with the on-chain population and the hardware-wallet population reported as their own denominators; the sector's own line is the share of exposed keys covered by the written address-rotation	Any quarter with no reduction on the custody population triggers workstream review; before closure every remaining entry has a funded treatment with a date or a SteerCo-signed exception, and every on-chain exception carries its protocol date and

KPI	Digital asset measurement	Threshold
	policy, with the value rotated to never-spent hash-protected outputs in the quarter	grade
New-system agility compliance	Percentage of new chain listings, custody integrations, wallet integrations and signing-stack deployments passing the CI/CD crypto-policy check and the provider-pattern review, and percentage of new custody, wallet and signing-stack arrangements that include the contractual crypto-agility clause with the acceptance-test rehearsal passed before go-live	Below 95% in any month triggers architecture and procurement governance review

RECOMMENDED IMMEDIATE ACTIONS

For organizations holding or managing digital assets at Maturity Levels 1 (Aware) and 2 (Initiated), these actions can begin immediately and do not depend on protocol readiness. Actions 1 to 8 are the sector's actions; actions 9 and 10 are the agility actions.

#	Action	Timeline	Phase
1	Quantify on-chain public key exposure across all chains, by exposure state, against a denominator enumerated from the treasury and custody records before the scan: 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	0–3 months	Phase 5

#	Action	Timeline	Phase
	does not make Bitcoin quantum-safe against future on-spend attacks.		
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 test environments that implement the rules	3–9 months	Phase 5

#	Action	Timeline	Phase
	under test (Bitcoin regtest or a custom Signet with a post-quantum signature scheme enabled, since a BIP-360 output type alone adds none; an interoperability devnet for Ethereum, with Sepolia for application-level tests) 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
9	Name a Crypto-Agility workstream owner in the function that controls the custody stack, the APIs and the release-signing pipelines, with a budget line from Year 1 and the agility-debt register as scope; name the Cryptographic Record owner and the protocol-governance seat beside them.	0–1 month	Phase 0

#	Action	Timeline	Phase
10	Schedule the first algorithm-change rehearsal: the key-establishment parameter-set change on the endpoint of action 4, or a key ceremony that generates a PQC-authorized signing key on the custody stack and retires it; time the four segments, roll it back, and file the timings as the first agility KPI reading and the first entry in the closure evidence.	3–9 months	Phase 5

FURTHER READING

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

- **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.
- **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.
- **Ethereum's Five Quantum Vulnerabilities – https://postquantum.com/quantum-threat-crypto/ethereum-quantum-vulnerabilities/ –** Account signatures, admin keys, EVM precompiles, PoS consensus, KZG commitments.
- **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.
- **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.
- **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.
- **Google Quantum AI Achieves 10x Reduction in Resources to Break Bitcoin's Cryptography – https://postquantum.com/security-pqc/google-quantum-bitcoin-ecdlp/ –** Analysis of the March 2026 whitepaper: 1,200 to 1,450 logical qubits, fewer than 500,000 physical qubits, the 18-minute runtime and the nine-minute primed-state window, and the on-spend, at-rest and on-setup taxonomy.
- **IonQ Compiles Shor's Attack on secp256k1 Down to 19,397 Ions and 26 Days per Attempt – https://postquantum.com/post-quantum/ionq-secp256k1-resource-estimate/ –** The September 8, 2026 analysis of IonQ's paper: the assumption ledger behind 1,457 logical qubits, 39 million Toffoli gates and 25.7 days per attempt, why the figures are specific to secp256k1, and what a weeks-per-key machine changes for exposed keys.

- **Beyond Bitcoin and Ethereum – Quantum Vulnerabilities – https://postquantum.com/quantum-threat-crypto/blockchain-ecosystem-quantum-vulnerabilities/ –** The May 2026 chain-by-chain reading behind the readiness subsection: post-quantum by design, migrating, and unaddressed.
- **Why Harvest Now, Decrypt Later Cannot Be Detected – https://postquantum.com/post-quantum/cannot-detect-harvest-now-decrypt-later/ –** The July 2026 analysis of why a passive collector leaves no evidence, and why the absence of evidence is not reassurance; on a public ledger the replica is the collection.
- **The Global PQC Migration Clock – https://postquantum.com/pqc-migration-timelines/global-pqc-migration-clock/ –** The maintained jurisdiction roster this extension's regulatory map points to, updated from the PQC Migration Brief.
- **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.
- **Rethinking CBOM – https://postquantum.com/post-quantum/rethinking-cbom/ –** Minimum Viable CBOM approach applicable to digital asset infrastructure.

APPENDIX J: REQUIREMENTS REGISTER

This register is generated from the text of this edition at each build and lists every statement in this extension that uses *must*. The four program-level provisions of the Universal Framework's Normative Convention bind this extension through its parent and are listed in the Universal's Appendix J; they are not repeated here. Every statement below binds inside the section that states it, and a statement that appears here without its section's conditions is read with them. The appendix letter matches the Universal's, so "Appendix J" names the requirements register in every document of the set.

Statements in document order

1. *Why Digital Assets Requires Its Own Extension.* Risk scoring must account for permanently exposed public keys that cannot be remediated because the private keys are lost.
2. *Digital Asset-Specific Challenges, Challenge 1: On-Chain Public Key Exposure.* Framework Impact: Phase 1 (Discovery) must include on-chain public key exposure analysis as a primary inventory track.
3. *Digital Asset-Specific Challenges, Challenge 1: On-Chain Public Key Exposure.* Phase 1 must record it as three separate claims: observed exposure state, reported key-control status and assessed migratability.
4. *Digital Asset-Specific Challenges, Challenge 1: On-Chain Public Key Exposure.* Phase 3 (Risk Scoring) must weight at-rest exposure by value concentration and key recovery feasibility, reading the observed exposure state and the value at risk as factors inside Dimension 2 (Phase 3 adaptation).
5. *Digital Asset-Specific Challenges, Challenge 2: Signature Size and Transaction Throughput.* Framework Impact: Phase 5 (Pilots) must include signature-size impact modeling on transaction throughput, fee economics, and state growth.
6. *Digital Asset-Specific Challenges, Challenge 2: Signature Size and Transaction Throughput.* Phase 6 (Infrastructure) must evaluate algorithm selection tradeoffs (ML-DSA security versus FN-DSA compactness) specific to blockchain constraints.
7. *Digital Asset-Specific Challenges, Challenge 3: Consensus-Level Migration Requires Coordinated Hard or Soft Forks.* For organizations holding digital assets

across multiple chains, each chain's governance model and PQC timeline must be tracked independently.

8. *Digital Asset-Specific Challenges, Challenge 3: Consensus-Level Migration Requires Coordinated Hard or Soft Forks.* Framework Impact: Phase 0 (Executive Mandate) must establish monitoring of consensus upgrade proposals across all chains in the organization's portfolio.

9. *Digital Asset-Specific Challenges, Challenge 3: Consensus-Level Migration Requires Coordinated Hard or Soft Forks.* Phase 4 (Roadmap) must track BIP/EIP/protocol-specific PQC timelines as external dependencies the organization cannot control, each graded for firmness, with the dependent on-chain entries shown against the dates that unblock them.

10. *Digital Asset-Specific Challenges, Challenge 4: Unmigrable Assets and Dormant Coins.* Institutional investors and custodians must model this scenario in their risk frameworks even if their own holdings are properly migrated.

11. *Digital Asset-Specific Challenges, Challenge 4: Unmigrable Assets and Dormant Coins.* 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.

12. *Digital Asset-Specific Challenges, Challenge 5: Smart Contract and DeFi 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.

13. *Digital Asset-Specific Challenges, Challenge 5: Smart Contract and DeFi Cryptographic Dependencies.* Phase 7 (Vendor Governance) must include DeFi protocol developers and smart contract audit firms in PQC readiness assessment.

14. *Digital Asset-Specific Challenges, Challenge 6: Proof-of-Stake Consensus Vulnerability.* Framework Impact: Phase 3 (Risk Scoring) must include PoS consensus integrity as a systemic risk category separate from individual key compromise.

15. *Digital Asset-Specific Challenges, Challenge 6: Proof-of-Stake Consensus Vulnerability.* Phase 4 (Roadmap) must track PoS chains' PQC consensus upgrade timelines.

16. *Digital Asset-Specific Challenges, Challenge 7: On-Setup Attacks and Zero-Knowledge Proof Systems.* The affected protocols must be replaced entirely; patching the cryptographic layer is insufficient because the compromise is in the public parameters themselves.

17. *Digital Asset-Specific Challenges, Challenge 7: On-Setup Attacks and Zero-Knowledge Proof Systems.* Framework Impact: Phase 3 (Risk Scoring) must classify on-setup vulnerabilities at the highest severity because they create permanent classical exploits.

18. *Digital Asset-Specific Challenges, Challenge 7: On-Setup Attacks and Zero-Knowledge Proof Systems.* Phase 5 (Pilots) must prioritize protocols with trusted setup dependencies for early migration.

19. *Digital Asset-Specific Challenges, Challenge 7: On-Setup Attacks and Zero-Knowledge Proof Systems.* Phase 7 (Vendor Governance) must ask every rollup, bridge and proof-system provider which specification its verifier implements, whether the transcript binding of every prover-supplied value has been reviewed against that specification, and which other deployed verifiers share the lineage.

20. *Digital Asset-Specific Challenges, Challenge 8: Privacy Chain Retroactive Deanonymization.* Framework Impact: Phase 3 (Risk Scoring) must account for retroactive privacy loss as an irreversible risk that cannot be mitigated by future migration.

21. *Digital Asset-Specific Challenges, Challenge 9: Exchange and Custodial Infrastructure.* 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.

22. *Digital Asset-Specific Challenges, Challenge 9: Exchange and Custodial Infrastructure.* 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), as separate entries.

23. *Digital Asset-Specific Challenges, Challenge 9: Exchange and Custodial Infrastructure.* Phase 6 (Infrastructure) must record every custodial HSM, KMS and multi-party signing stack in the four-field register with its entropy references.

24. *Digital Asset-Specific Challenges, Challenge 9: Exchange and Custodial Infrastructure.* Phase 7 (Vendor Governance) must include blockchain node software providers, wallet SDKs and multi-party signing providers, agility questions first.

25. *Digital Asset-Specific Challenges, Challenge 10: Tokenized Real-World Assets and Stablecoins.* Phase 3 (Risk Scoring) must evaluate host chain PQC readiness for every tokenized asset in the portfolio.

26. *Alignment with Universal Framework v3.0, SP 800-208 for Firmware and Release Signing.* 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.

27. *Alignment with Universal Framework v3.0, SP 800-208 for Firmware and Release Signing.* A signing service that does not meet section 8 is not a conforming deployment, and the verifiers must accept the parameter set chosen.

28. *Phase 5 adaptation.* The constraint is that the particular network used must implement the proposed verification rules.

ABOUT

ABOUT THE AUTHOR

Marin Ivezic is a former Fortune Global 500 CISO/CTO, the founder and CEO of Applied Quantum, and the founder of Quantum Academy (QuantumAcademy.com). PostQuantum.com is his personal blog. 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 standards, products and deadlines change, and the book supplies the depth that a methodology document omits by design.

QUANTUM ACADEMY

Quantum Academy (QuantumAcademy.com), founded by the author, offers trainings and certifications on the topics this framework covers, from executive education on quantum risk to practitioner courses on PQC migration, crypto-agility and cryptographic inventory, for the roles and training levels described in Skills & Team Structure.

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