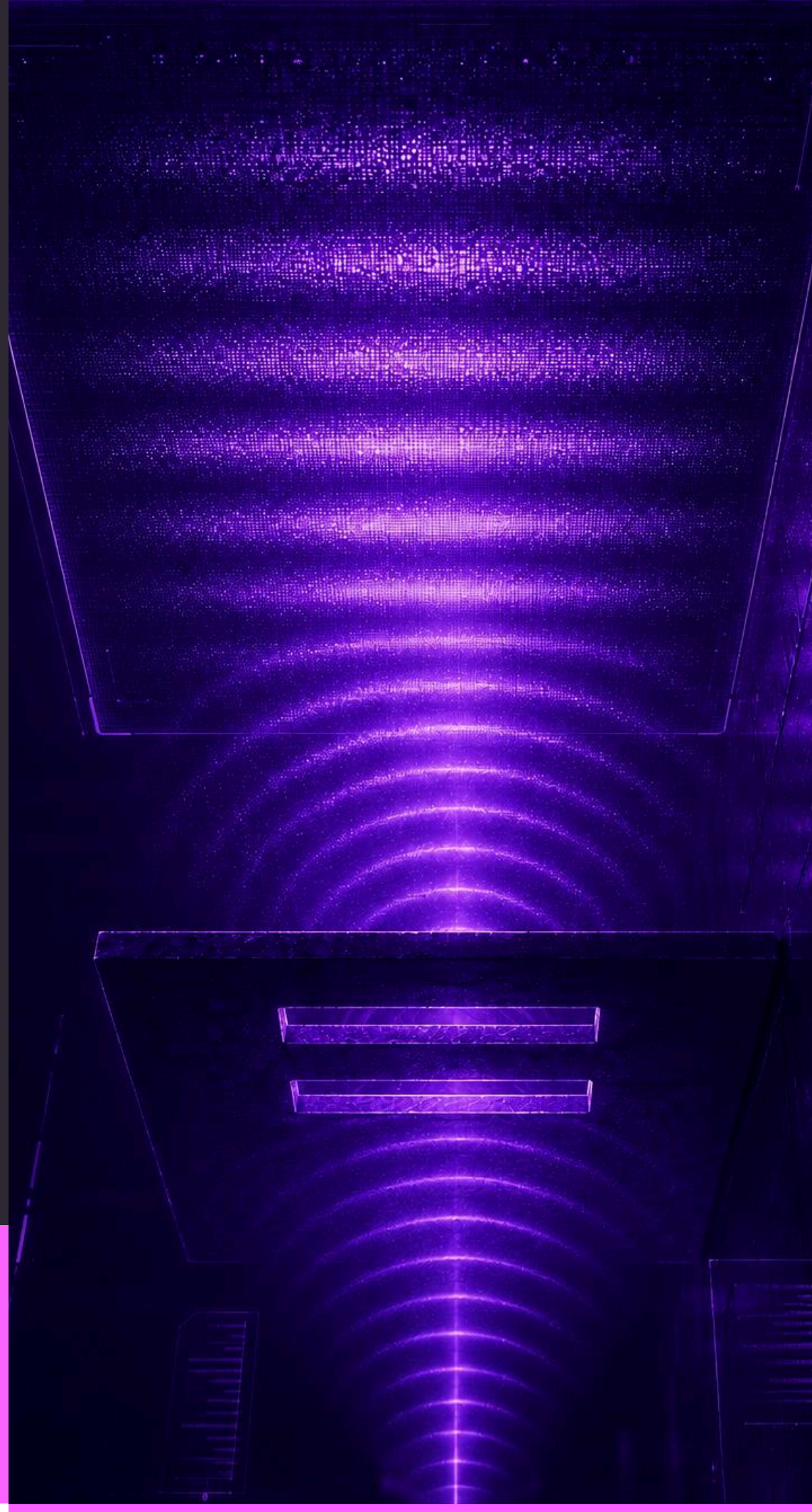
TAURUS



June 2026

Quantum Computing Risk in Digital Asset Custody: HSM vs. MPC

A practical guide to managing the post-quantum transition in institutional digital asset custody

TAURUS

Table of Contents

TAURUS

Foreword

"Our world is dominated by the extreme, the unknown, and the very improbable—and all the while we spend our time engaged in small talk".

Nassim Nicholas Taleb wrote these words in The Black Swan: The Impact of the Highly Improbable (2007), just before the global financial crisis validated his thesis in the most dramatic fashion. His central argument—that humans are structurally ill-equipped to anticipate black swans: rare, unanticipated, high-impact events—remains as relevant as ever. We build our models on what we know, anchor our decisions to historical precedent, and systematically underestimate what lies beyond the edge of our experience.

Fortunately, the quantum computing risk has been debated for decades, and its impact is very clear. There is broad consensus on the adverse consequences of Q-day catching our systems unprepared, yet the conversation too often devolves into a dispute over timing. Skeptics point to historical patterns and technical constraints to argue the threat will not materialize within our lifetimes. Others cite accelerating research to warn it may arrive far sooner than expected, as early as 2029.

The honest answer is that nobody knows. But uncertainty about timing is not an argument for inaction —it is precisely the argument for preparation.

The potential impact on our security, financial systems, and critical infrastructure is too significant to leave to chance. A post-quantum world is coming. The only open question is whether we will be ready when it arrives.

At Taurus, we chose to act early and are ready for the post-quantum era. We have been preparing for Q-day since 2021, and have shared our thinking publicly since 2023—from risk assessment frameworks to the post-quantum technology landscape and the latest advances in efficient post-quantum signatures (Quantum doomsday planning 1 and 2, Faster PQ signatures). This publication continues that work.

You can be ready too.

1. Introduction

Blockchains run on public-key cryptography. Every transaction depends on mathematical problems that a sufficiently capable quantum computer could solve. That machine does not exist yet. But the standards to replace vulnerable algorithms already exist and governments are publishing guidelines and deadlines for their critical infrastructure to migrate, as do the main blockchains (check BIP-360 for Bitcoin, pq.ethereum.org for Ethereum).[1]

Three things justify acting early against the quantum computing risk.

- **First, the tools exist.** NIST published its first post-quantum standards in August 2024, and those algorithms already ship in major cloud platforms, programming languages, and security libraries.
- **Second, the deadlines are set.** For example, NIST IR 8547 deprecates RSA, ECDSA, and elliptic curve Diffie-Hellman after 2030 and bans them after 2035.
- **Third, the risk is pervasive and not in the future.** Adversaries can record encrypted traffic today and decrypt it later, once a capable quantum computer is available. Confidential data with a long shelf life is at risk right now. Waiting for hardware milestones before acting is not sound risk management.[2]

Industry roadmaps are now translating these requirements into operational migration plans. Circle's roadmap for Arc and USDC, for example, treats post-quantum readiness as a stack-wide issue rather than a transaction-signature replacement alone, covering smart contracts, privacy, infrastructure, vendor dependencies, custody and key management, and account recovery. [3]

This paper targets institutions that are already active in the digital asset space or planning to enter it with a solid security posture. It provides a practical framework for assessing quantum risk and evaluating post-quantum readiness across the digital asset custody stack—focusing on what can be acted on today: cryptographic inventory, HSM and MPC dependencies, quantum-safe connectivity, long-term backup exposure, policy integration, vendor readiness, and crypto agility.

The paper also offers clear guidance on the post-quantum posture of HSM versus MPC architectures, and identifies a fundamental mathematical barrier to MPC compliance under certain post-quantum requirements (see Section 3.5).

The paper is organized as follows. Section 2 explains the core quantum risks for digital asset custody. Section 3 summarizes the relevant standards, timelines, hybrid approaches, and infrastructure readiness. Section 4 provides a practical migration plan built around five steps: observe, assess, decide, communicate, and act and monitor. Section 5 outlines Taurus' post-quantum readiness work. Section 6 concludes with the main priorities for institutions.

1. https://github.com/bitcoin/bips/blob/master/bip-0360.mediawiki; https://pq.ethereum.org/
2. https://www.aumasson.jp/data/talks/pqcbha26.pdf; https://www.taurushq.com/blog/quantum-computers-taurus-is-ready/; https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf
3. https://community.arc.io/public/blogs/circles-post-quantum-security-roadmap-securing-blockchains-smart-contracts-and-digital-assets-for-the-quantum-era-2026-05-30

2. The quantum computing risk

2.1 What quantum computing changes

A quantum computer is not a faster version of a classical computer. It does not work by trying all possible answers at once. It uses quantum mechanics to efficiently solve a small number of specific problems. The two problems relevant to cryptography are factoring large integers and computing discrete logarithms.

RSA, Diffie-Hellman, and all elliptic-curve cryptography standards depend on one of those two problems. Classical computers cannot solve them at real-world key sizes, which is what makes the cryptography secure. A large enough quantum computer running Shor's algorithm could break the mathematical foundation of most deployed public-key cryptography: transaction signing, TLS, SSH, key wrapping, code signing, PKI.

No such quantum computer exists today. Current machines are research prototypes at around 100 qubits, which is nowhere near the capability needed to break real cryptography. The timeline is genuinely unknown, and hard to predict. Nobody can tell when a cryptographically relevant quantum computer will exist. It could be a Tuesday or a Saturday, it could be the 2030s, the 2060s, or never. Our view: before 2040 is unlikely based on current evidence. But that uncertainty is not a reason to wait, because of the high impact of the risk and the long migration timelines. Addressing the quantum computing risk is... risk management, not guesswork.

Recent developments

Two papers published on March 30, 2026 brought the topic into many boardrooms for the first time:

- First, Google Quantum AI disclosed that it had reduced the theoretical number of quantum gates needed to break elliptic curve cryptography. The underlying technique builds on a French academic paper (IACR ePrint 2026/280) that reduced the qubit count for discrete logarithms on elliptic curves. The actual algorithm remains undisclosed; evidence was provided as a zero-knowledge proof. The claimed estimate is execution in minutes using fewer than half a million physical qubits. No quantum computer near that scale exists today, but the hardware gap to a cryptographically relevant machine is narrowing.[4]
- Second, a theoretical paper describes a quantum computing architecture allowing Shor's algorithm to run with as few as 10,000 reconfigurable atomic qubits, using a neutral-atom architecture. This is a hardware-architecture claim only; no physical implementation exists. A related 2025 experiment involved 6,100 neutral-atom qubits, though without entanglement or error correction, two crucial components of a quantum computer.[5]

Both results point in the same direction: the gap between today's prototypes and a cryptographically relevant machine is narrowing. Waiting for confirmed milestones before acting is not sound risk management.

4. https://quantumai.google/blog/2026/safeguarding-cryptocurrency; https://eprint.iacr.org/2026/280
5. https://arxiv.org/abs/2503.24187

2.2 Impact on IT security systems

As far as information security is concerned, quantum computing mostly affects public-key cryptography based on RSA and elliptic curves (simplifying a bit). It does not affect symmetric cryptography such as the AES cipher or the SHA-2 and SHA-3 hash functions.[6]

The exposure of IT systems such as digital asset custody falls into three areas, depending on the component concerned:

- **Signature and authentication.** Blockchain transaction signatures, cryptographic entitlements, SSH host keys, client certificates, code signing, firmware signing, software package signing, and certificate chains.
- **Key establishment and encryption key protection.** TLS, SSH, IPsec, WireGuard, end-to-end encrypted messenger, PGP, S/MIME, ECIES, and key wrapping schemes.
- **Advanced cryptographic protocols.** Protocols such as those performing multi-party computation, zero-knowledge proofs, password-authenticated key exchange, and anonymous credentials often rely on the hardness of factoring or discrete logarithms, directly or indirectly, making them vulnerable to quantum computers.

Most blockchains use elliptic curve signatures: Bitcoin supports ECDSA and Schnorr signatures, while Ethereum uses ECDSA for transactions and BLS signatures at the consensus level. When you broadcast a transaction, you publish the corresponding public key—because it's necessary to verify the signature. A quantum computer running Shor's algorithm could recover the private key from that public key and therefore forge transactions on your behalf, potentially with ill intent. The less visible risk is the custody control plane. Even if you cannot migrate blockchain signatures yet, you can and should improve transport security, backups, authentication, vendor integrations, and software supply-chain controls right now. This is because even after you've properly migrated to post-quantum blockchain signatures, an attacker may have gained a foothold in your network because of other quantum-unsafe systems.

Conflating these two types of exposure leads to wrong priorities. Encryption and key exchange are vulnerable to a **harvest-now-decrypt-later attack:** an adversary records your encrypted traffic today, stores it, and waits. Once a capable quantum computer exists, they may decrypt what they collected. Any data that must stay confidential for years is at risk right now. Signatures are different. A signature on a past transaction cannot be retroactively forged in a useful way. The risk from signatures is about future transactions, not historical ones. Prioritize accordingly: transport encryption and backups first, blockchain transaction signing when the ecosystem is ready.

6. https://words.filippo.io/128-bits/

2.3 What is not the immediate problem

Symmetric cryptography does not need to change. This is a common source of confusion, so it is worth being direct about it.

The confusion comes from Grover's algorithm. Grover speeds up searching, and in theory it halves the effective security of symmetric keys. But this view is an oversimplification and would not effectively reduce AES-128's security from 128- to 64-bit security. NIST, and the cryptography community broadly, agree: AES-128 and SHA-256 are safe, for example. No compliance mandate requires larger symmetric key sizes. You do not need to change symmetric cryptography as part of post-quantum migration.

2.4 The blockchain constraint

Before covering the technical details of post-quantum migration in custody, there is one structural constraint that has no equivalent in most enterprise security programs. It is specific to digital asset custody, and understanding it is essential for setting realistic expectations about what post-quantum readiness means in this context.

A bank can update its TLS stack this quarter to serve quantum-safe connections. Making Bitcoin or Ethereum accept a new signature scheme requires protocol changes, wallet updates, node operator consensus, and client migration. No single institution can arrange that.

No custody provider can honestly claim “full” post-quantum coverage today as they all depend on the underlying blockchain protocols. The realistic objective is to make every layer you control ready, keep your architecture crypto-agile, monitor blockchain developments, and migrate on-chain when the ecosystem gets there. This is what Taurus did.

To understand why this matters, consider how a blockchain transaction works. When a custodian signs a transaction and broadcasts it to the Bitcoin or Ethereum network, the network validates the signature using the rules of its own protocol. Bitcoin currently accepts secp256k1 ECDSA and Schnorr signatures. Ethereum currently relies on secp256k1 ECDSA-based transaction signatures. The network does not care what HSM or MPC system produced the signature. It only checks that the signature is valid under the scheme it expects. So even if Taurus, or any other wallet provider, deploys post-quantum signing infrastructure today, it cannot submit post-quantum signatures to Bitcoin or Ethereum. The network would reject them. This is the constraint that makes blockchain custody different from every other enterprise security migration: the endpoint that validates your signatures is outside your control, and it will not accept new signature formats until the entire ecosystem around it agrees to change.

There is a useful framing here, sometimes called the “quantum gravity principle”: a computer that could break Bitcoin would almost certainly not be used to steal it. If such a machine became known, prices would collapse before any theft occurred. A nation-state with that capability would have far more valuable targets. This does not reduce urgency. It helps prioritize: the biggest near-term risks are harvest-now-decrypt-later attacks on confidential data, and longer-term weakening of authorization controls.

2.5 MPC: the good, the bad, and the ugly

MPC can make key compromise harder, but it does not change the signature scheme accepted by the blockchain. If the network validates ECDSA or EdDSA, the final on-chain security still depends on elliptic curve cryptography. Distributing the signing process does not change that.

A common assumption about MPC is that distributing signature computation across multiple systems reduces risk, such as a single-point compromise risk—but it does not reduce quantum risk, creates new risks, and the distinction is worth understanding clearly.

The good: A well-designed MPC-based custody architecture requires an attacker to attack and compromise multiple systems rather than a single one. In practice, this leads to the age-old security dilemma of having to choose between 1) maintaining and protecting multiple systems or secrets and 2) focusing on a single very strong type of system.

Also, MPC does not transform quantum-vulnerable signatures into quantum-safe ones. In the context of signatures, an MPC protocol achieves exactly the same computation as the signature scheme, just distributing the work over multiple systems. MPC cannot, by itself, make Bitcoin, Ethereum, or other classical-signature blockchains quantum-safe.

The bad: MPC also carries its own attack surface that has been covered extensively. The signing protocol, its cryptographic subprotocols (such as zero-knowledge proofs), participant authentication channels, and their respective endpoints can all rest on classical cryptographic assumptions, and have flaws on their own. If any of these break, the MPC system is compromised even if the on-chain signature scheme remains intact. MPC's cryptographic dependencies should therefore be assessed independently from blockchain signing.[7]

The ugly: Finally, MPC protocols may not support post-quantum signatures the way HSMs already do (see Section 3.5 below). While some post-quantum signatures can theoretically be computed in an MPC setting, the relevant protocols (for example for ML-DSA) are very recent (2025–2026) and have not yet been validated for production use. Others—most notably SLH-DSA and its variants, which is under consideration by major blockchain protocols including Ethereum—are mathematically incompatible with MPC computation (see Section 3.5). Institutions entering or planning to enter the digital asset space should weigh this structural limitation carefully.

7. https://www.taurushq.com/reports/air-gapped-cold-storage-architectures/

3. Benchmark standards and market direction

3.1 NIST post-quantum standards

The U.S. agency NIST has led the global post-quantum standardization effort since 2016, running a public competition similar to the ones that produced AES and SHA-3. The NIST standards are the de facto global reference for financial institutions, vendors, and regulators.

Three post-quantum cryptography standards are fully specified, as of June 2026.

- ML-KEM (FIPS 203) for key agreement, where two parties establish a shared secret without sending the key over the channel.[8]
- ML-DSA (FIPS 204) is a signature algorithm based on lattice problems, which are believed hard for quantum computers to solve.[9]
- SLH-DSA (FIPS 205) is a signature algorithm based on hash functions that have been studied for decades and do not depend on factoring or discrete logarithms.[10]

Knowing these matters for a practical reason: they will determine what vendors support, what your policies need to require, and what auditors will ask about. The FIPS numbers (203, 204, 205) are document identifiers in the same series as AES (FIPS 197) and SHA-256 (FIPS 180).

Standard	Function	Practical relevance for custody
FIPS 203 / ML-KEM	Key encapsulation	Hybrid or post-quantum key establishment for transport, APIs, and service-to-service channels.
FIPS 204 / ML-DSA	Digital signature	Post-quantum signatures for software, documents, attestations, and future protocol support.
FIPS 205 / SLH-DSA	Stateless hash-based signature	Conservative hash-based signature option. Much slower than ML-DSA but relies on well-studied hash function security rather than lattice assumptions. Best suited to signing long-lived artifacts such as certificates, firmware, and audit records rather than high-frequency transaction signing.
FIPS 206 / FN-DSA	Digital signature (standard specification in progress)	Compact lattice-based signature. Smaller than ML-DSA. Useful where bandwidth or storage is constrained.
HQC	Key encapsulation (standard specification in progress)	Code-based KEM. Provides algorithmic diversity alongside ML-KEM. Useful as a backup if lattice assumptions are ever weakened.

8. https://csrc.nist.gov/pubs/fips/203/final
9. https://csrc.nist.gov/pubs/fips/204/final
10. https://csrc.nist.gov/pubs/fips/205/final

3.2 Hybrid cryptography

A hybrid scheme runs a classical and a post-quantum algorithm together. Security holds as long as either one is secure. This is often the recommended approach during the transition: you get quantum protection without betting entirely on newer algorithms that have less real-world deployment history. Hybrid schemes are particularly recommended for KEMs, because once confidentiality is lost you can't get it back, whereas signature keys can be revoked. For key agreement, hybrid schemes typically combine X25519 Diffie-Hellman with ML-KEM. The shared secret is derived from combining both outputs. An attacker needs to break both systems, which could involve a capable quantum computer (for X25519) and the ability to break ML-KEM or its software. Hybrid schemes are especially relevant for secure channel protocols such as TLS and SSH, as used in service-to-service communication, API channels, and infrastructure connectivity. The IETF standardized ways to integrate post-quantum crypto into such protocols.[11]

Size trade-offs

Post-quantum algorithms tend to have larger keys and payloads. In terms of speed, ML-KEM and ML-DSA are comparable to ECDH and ECDSA but SLH-DSA is orders of magnitude slower.

Size (bytes)	ECDH P-256	ML-KEM-512 (PQ)	HQC-128 (PQ)
Public key	64	800	2,249
Private key	32	1,632 (64 compressed)	2,289
Ciphertext	65	768	4,481

KEM size comparison. ML-KEM private keys can be stored as a 64-byte seed.

Size (bytes)	ECDSA P-256	ML-DSA-44 (PQ)	SLH-DSA-128s (PQ)
Public key	64	1,312	32
Private key	32	2,528 (32 compressed)	64
Signature	64	2,420	7,856

Signature size comparison. SLH-DSA's 7.9 KB signature has throughput implications at scale.

11. https://github.com/veorq/awesome-post-quantum#ietf-standards-and-proposals

3.3 Transition timelines

At the time of writing, most major public-sector plans target broad deployment by 2030-2040. Financial institutions may not be directly subject to those deadlines, but the deadlines shape vendor roadmaps, audit expectations, and client questionnaires regardless of whether you are a federal agency.[12]

NIST IR 8547, "Transition to Post-Quantum Cryptography Standards," sets explicit dates. ECDSA, EdDSA, and RSA are deprecated after 2030 and disallowed after 2035. Elliptic curve DH follows the same schedule. For US federal agencies these deadlines are mandated by OMB M-23-02 and NSM-10 and enforced by CISA. Institutions elsewhere should treat these timelines as a leading indicator of global regulatory direction.

The practical implication is simple: you need a documented plan, a roadmap that is owned and reviewed is worth far more than assuming your vendors will sort it out.[13]

3.4 Digital infrastructure readiness

Post-quantum support is spreading faster than many custody teams expect. Cloudflare estimates that post-quantum HTTPS already accounts for over 60 percent of web traffic in Singapore and over 70 percent in Japan, driven by browser and CDN support for hybrid TLS. Cloud KMS services, operating systems, and open-source libraries are adding support steadily. HSM signing and MPC protocols are less mature but advancing.

In aggregate:

- **Deploy now**: hybrid TLS/VPN, backup encryption, cloud API channels.
- **Pilot now:** HSM PQC signing, MPC protocol review, code signing.
- **Monitor actively:** public blockchain migration, HSM FIPS 140-3 PQC validation.

3.5 Signature scheme readiness – HSM vs. MPC

This section, including the table on the next page, captures one of the paper's central insights: HSM and MPC architectures do not share the same post-quantum migration path or readiness profile.

Tier-1 HSMs (such as those of Thales) already support post-quantum signature algorithms within a protected hardware boundary—subject to firmware version. MPC, by contrast, requires a practical threshold protocol for each relevant signature family before it can support that scheme at all. This distinction determines what can be deployed today, what may become production-ready over time, and what is structurally difficult or impossible to support regardless of vendor roadmap.

12. https://csrc.nist.gov/pubs/ir/8547/ipd; https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/; https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF
13. https://www.cisa.gov/sites/default/files/2024-09/Strategy-for-Migrating-to-Automated-PQC-Discovery-and-Inventory-Tools.pdf

This is already visible in emerging blockchain roadmaps. For example, Circle's roadmap for Arc selects SLH-DSA-SHA2-128s, a NIST hash-based signature scheme, for smart-account verification, while keeping native Arc transaction signatures ECDSA-only in the near term because of throughput, standardization, and hardware-wallet constraints. Aptos has proposed the same scheme for post-quantum accounts. If such schemes become part of blockchain migration paths, custody architectures will need to support them; this is straightforward for HSM-based systems, but much more constrained for MPC-based systems.

In particular, there is a fundamental mathematical barrier to MPC readiness when hash-based signatures, which are under consideration by Ethereum and other large blockchains, are involved: due to the lack of algebraic structure in the underlying hash functions, no such structure can be leveraged to distribute the signature computation while satisfying the constraints of completeness, correctness, and privacy, as demonstrated in recent research.[14]

PQ signature family	Examples	Selected by	HSM	MPC
Lattice-based signatures	ML-DSA (Dilithium) FN-DSA (Falcon)	-	✅ (built-in or via FM)	⚠ (possible, but needs time for production readiness)
Hash-based signatures	SLH-DSA / SPHINCS+, LMS/HSS	Circle, Circle Arc, Aptos, Ethereum[15]	✅ (built-in or via FM)	⚠ (theoretically impossible)
Multivariate	No standard yet, NIST candidates MAYO, QR-UOV, SNOVA, UOV	-	✅ (built-in or via FM)	⚠ (most MPC-friendly, needs time for readiness)
MPC-in-the-head	NIST candidates MQOM, SDitH, South Korean standard AIMer	-	✅ (built-in or via FM)	⚠ (not MPC-friendly, needs more research)

Legend for the table

✅ easily supported with no new material risk

⚠ possible in principle, but not generally available in production-grade custody implementations, and introducing new risks related to the protocol adopted

❌ impossible to support, due to the mathematical structure of the scheme

14. https://csrc.nist.gov/csrc/media/presentations/2026/mpts2026-4b4/images-media/mpts2026-4b4-slides-bbts-hbs-kumar.pdf
15. https://community.arc.io/public/blogs/circles-post-quantum-security-roadmap-securing-blockchains-smart-contracts-and-digital-assets-for-the-quantum-era-2026-05-30; https://strawmap.org/

4. Managing migration

Post-quantum migration should not be considered a project with a fixed completion date. Legacy cryptography may stay in production alongside post-quantum controls for years. Standards will evolve. Vendors will certify new capabilities. Blockchains will migrate on their own schedules—likely by 2029 or before. The five-step approach below is an iterative loop, not a linear sequence, and is directly inspired by the OODA loop model from U.S. Air Force Colonel John Boyd.

Migration plan approach

Observe -> Assess -> Decide -> Communicate -> Act & monitor

4.1 Observe

Build an inventory of the places where public-key cryptography is used, with a reasonable level of detail. This cannot be done from memory or from vendor documentation alone. It requires reviewing live configurations, firmware versions, and integration specifications. The goal is a specific, named list of systems with an assigned owner for each, not a general category.

There are many areas and systems to cover: blockchain transaction signing and the signature schemes in use; HSM key types and firmware versions; MPC protocol dependencies; TLS, SSH, IPsec, and VPN configurations; internal PKI; administrator authentication and approval tokens; software and firmware update channels; code signing; backup encryption and key wrapping; client API authentication; third-party integrations; software updates; and disaster recovery infrastructure, to cite a few. For internal systems, documentation review and configuration audit may be enough. For vendors, verify claimed post-quantum support on live systems and ask for a formal roadmap where support is missing.

Once the inventory is complete, you may prioritize according to two dimensions: the impact of quantum computing attacks (in terms of assets, breadth of impact, compliance, etc.), and how hard it is to migrate. The goal is to sort systems into three groups: upgrade now, pilot, or accept the residual risk with a defined review date.

4.2 Assess

The assessment mainly consists of prioritizing systems based on risk and cost, and then documenting the remediation strategies proposed. There is no single perfect model or framework, and most likely your organization already has one that your teams are used to.

4.3 Decide

With the assessment done, turn it into explicit decisions. Which systems need action now? Where should hybrid or non-hybrid schemes be deployed? Which vendors need roadmap commitments written into their contracts? Which HSM features should enter a test environment? Which MPC subprotocols need a cryptographic audit? Which blockchain assets need migration watchlists? Which policies need to be updated? And which internal deadlines align with NIST's 2030 deprecation and 2035 disallowance schedule?

If a system is not being migrated yet, make that an explicit, documented decision. Inaction by default is not the same as consciously accepting the risk.

4.4 Communicate

Post-quantum readiness requires communication to several audiences, each with different needs.

- **Internal audiences.** Board and executive updates, engineering guidance, risk, and compliance documentation, procurement requirements and operational runbooks.
- **External audiences.** Client-facing roadmap summaries, enterprise security documentation, regulator or auditor responses, vendor coordination plans and ecosystem participation where blockchain protocol upgrades are relevant.

The message should be calibrated. Systems are not suddenly unsafe, but the cryptographic assumptions they rely on are changing, and the institution has a structured plan to address that.

4.5 Act & monitor

This is when changes—and their unintended consequences—happen. When deploying hybrid transport where available, updating cryptography and key management policies, or testing HSM post-quantum features, for example. As in any IT project, expect the unexpected.

Apparent readiness does not mean you are done. As new products are developed, as commits are written, as new vendors are onboarded, quantum-unsafe cryptography may sneak back in. You should have processes to catch those as early as possible.

5. Taurus' post-quantum readiness

Taurus started its post-quantum program in 2021.

As of 2026, our VPN and secure channel protocols are migrated to post-quantum key agreement (hybrid DH/KEM), including Cloudflare Tunnel virtual networking, SSH services and clients, and TLS (using the 1.3 post-quantum extension).

What is not migrated includes the off-chain transaction intent endorsements (as we await YubiKey support), and, of course, blockchains.

Taurus has actively contributed to post-quantum awareness through public writing, technical presentations, and ecosystem monitoring. This includes articles on quantum risk assessment and post-quantum technology, public presentations on proactive mitigation, and curated references for post-quantum cryptography tools, standards, and research.

6. Conclusion

Post-quantum cryptography is not a reason to panic. It is a reason to act. The algorithms exist. The standards are published. The tools are available. What remains is the institutional work: building a cryptographic and systems inventory, prioritizing said systems based on risks, engaging vendors, updating policies, and putting together a roadmap that holds up when auditors, clients, and regulators ask about it.

For custody, that work starts with the inventory. HSMs and MPC signature layers are central, but they cannot be evaluated in isolation.

- MPC shows structural weaknesses vs. HSM, as MPC architectures are not able to support hash-based signatures and will likely never be able to support them, due to mathematical constraints.
- Transport security, PKI, code signing, approval workflows, backup procedures, and vendor infrastructure all need to be in scope.

Taurus started this work in 2021. The controls already deployed include a cryptographic inventory, post-quantum hybrid VPN, quantum-safe backup encryption, updated policies, and a crypto-agile Taurus-PROTECT architecture.

The goal is clear: protect every layer you control, reduce confidentiality risk now, and build the governance to act quickly when blockchains get there (by or before 2029). Institutions that handle this well will be those that built cryptographic agility in from the start, not those that bolted it on later.

Appendix

Appendix 1:
Example post-quantum readiness questions for HSM vendors

1. Which post-quantum algorithms are supported today?
2. Are ML-KEM, ML-DSA, or SLH-DSA supported?
3. Is support available in production, preview, or roadmap only?
4. Is support included in certified modules?
5. What firmware versions are required?
6. Can post-quantum keys be generated inside the HSM boundary?
7. How are post-quantum private keys backed up and restored?
8. Are post-quantum operations available through existing APIs?
9. What are the expected performance characteristics?
10. How are audit logs and administrative operations protected?
11. What is the roadmap for post-quantum code signing and firmware signing?
12. What migration support is available for existing clients?

Appendix 2:
Example post-quantum readiness questions for MPC vendors

1. Which signature schemes are currently supported?
2. Which blockchain signature formats are supported?
3. Does the protocol rely on elliptic curve assumptions internally?
4. Which public-key primitives are used for participant authentication?
5. Which secure channel protocols are used between MPC participants?
6. Are any zero-knowledge, commitment, or oblivious transfer subprotocols used?
7. Is there a roadmap for post-quantum threshold signatures?
8. Are post-quantum schemes available in production or research only?
9. How are key shares generated, refreshed, backed up, and recovered?
10. Can the platform support hybrid or migration workflows?
11. How are clients expected to rotate wallets or addresses when blockchain protocols evolve?
12. What third-party audits cover the cryptographic protocol?

Appendix

Appendix 3:
Example decision tree for custody teams

Question	Action
Does the system use RSA or elliptic curve cryptography?	**If yes,** add it to the post-quantum inventory.
Does the system protect long-lived confidential data?	**If yes,** prioritize key agreement, encryption, and key wrapping controls.
Does the system authorize asset movement?	**If yes,** prioritize transaction signing, policy enforcement and approval workflows.
Can the system be upgraded independently?	**If yes,** plan internal migration or pilot deployment. If no, identify vendor, regulator, or protocol dependencies.
Is post-quantum support available today?	**If yes,** test in a controlled environment. If no, document residual risk and obtain a roadmap.
Is the control production-ready, certified, and operationally supportable?	**If yes,** include it in the deployment roadmap. If no, keep it in pilot or monitoring status.

Appendix 4:
Practical first steps

1. Create a custody-specific cryptographic inventory.
2. Add post-quantum readiness to vendor due diligence.
3. Review HSM and MPC roadmaps.
4. Enable hybrid key agreement where supported and appropriate.
5. Protect long-term backups with quantum-safe cryptography.
6. Pilot post-quantum signing for non-blockchain workflows.
7. Update cryptography and key management policies.
8. Build blockchain-specific migration watchlists.
9. Report progress through the existing risk governance process.

TAURUS

Contact

contact@taurushq.com ■ https://www.taurushq.com