FRANKLIN TEMPLETON

Perspective from Franklin Templeton Digital Assets

# Digital asset security in the quantum era

November 2025 | White Paper


## Executive Summary

Quantum computing is one of the few foreseeable technologies capable of reshaping the security, custody, and valuation framework of digital assets. While still in its formative stage, its progress now demands proactive attention from institutional investors and digital infrastructure providers.





**Priti Kumari**
Research Analyst
Franklin Templeton Digital Assets





**Christopher Jensen**
Head of Research
Franklin Templeton Digital Assets


## 1. The Material Risk

Quantum computers capable of breaking today's public-key cryptography (e.g., RSA-2048, ECDSA/EdDSA) remain in development, but credible estimates place that milestone—"Q-Day"—within the next 5-8 years, with uncertainty driven by progress in fault-tolerant logical qubits rather than raw qubit counts. When achieved, Shor's algorithm could derive private keys from exposed public keys, undermining asset ownership across blockchains, custody systems, and authentication protocols. Grover's algorithm modestly reduces hash security but does not endanger proof-of-work consensus mechanisms.

## 2. Differential Impact Across the Digital Asset Stack

- **Bitcoin:** Vulnerability depends on address format and key exposure.
  - **High risk:** Legacy P2PK and reused P2PKH addresses.
  - **Moderate risk:** P2SH and multi-sig implementations.
  - **Low risk:** SegWit and Taproot, which conceal public keys until use and allow future migration.
- **Smart-Contract Platforms (ETH, SOL, ADA):** Signature schemes require post-quantum upgrades, achievable through upgradeable contract architectures.
- **Stablecoins & Tokenized Assets:** Issuer key rotation and contract agility are critical to secure collateral and preserve parity.
- **Custodians, Exchanges & Bridges:** Exposure lies in TLS, VPNs, and code-signing; hybrid PQC adoption and crypto-agile governance are the mitigants.

## 3. Institutional Response and Strategic Readiness

Global finance is mobilizing for post-quantum security.

- **NIST** has standardized Kyber and Dilithium, adding HQC (2025) for algorithmic diversity.
- **NSA's CNSA 2.0** mandates ML-KEM and SLH-DSA by 2025, with full adoption by 2030, and warns of "Harvest Now, Decrypt Later" risks.
- **FS-ISAC and IETF** are coordinating hybrid-TLS pilots (2025–26) and PQC internet standards.
- **Google, Cloudflare, and Akamai** run live PQC-TLS; HSBC, JPMorgan, and Wells Fargo test QKD interbank links.
- Custodians like **Coinbase, Fireblocks,** and **Anchorage** are adopting hybrid PQC stacks and automated key rotation.
- Post-quantum migration is now institution-led, with a 2030 quantum-safe target.


Not FDIC Insured | No Bank Guarantee | May Lose Value

## 4. The Investment Implication

Quantum risk is a duration risk—its realization timeframe is uncertain, but its impact on confidence, custody assurance, and key-management integrity is absolute once realized. Allocators should evaluate counterparties on three axes:

- **Cryptographic Agility:** Ability to rotate keys, swap algorithms, and coordinate upgrades.
- **Governance Readiness:** Capacity to execute protocol-level migrations securely.
- **Disclosure Discipline:** Transparent inventory of cryptographic dependencies.
- **Valuation channel:** As crypto-agility becomes verifiable, assets and counterparties that can rotate keys, swap algorithms, and coordinate upgrades should command lower operational risk premia and tighter spreads, while legacy exposures face a migration discount. We expect an emerging "PQ-premium" for quantum-ready custody and networks as disclosures and pilots turn into production deployments

## 5. Strategic Outlook

The digital asset ecosystem exhibits clear strengths—early standardization, hybrid pilots, and embedded agility—but also faces weaknesses in legacy migration cost and regulatory fragmentation. The opportunity lies with first movers who convert crypto agility into fiduciary advantage and market quantum-secure custody as a differentiator, while the threats stem from asynchronous rollouts or sudden quantum breakthroughs compressing migration timelines.

The quantum transition is less a countdown to crisis than a test of operational excellence and foresight. Institutions that prepare now will preserve trust and capture the premium flows of the quantum-secure era.

## Quantum Computing Fundamentals and the Road to Q-Day

Quantum computing is an emerging form of computation that applies the principles of quantum mechanics to process information beyond the limits of traditional computers. Instead of using bits that represent either 0 or 1, quantum computers use qubits or quantum bits. A qubit can exist in a combination of both 0 and 1 at once due to a property known as superposition. When multiple qubits interact, they can also become entangled, meaning the state of one qubit is linked to the state of another even when they are far apart.

The field of quantum computing is best viewed through six research domains as shown in the following table: *Quantum Computing Research Domains*

### Table 1: Quantum Computing Research Domains

| **Domain** | Example Algorithms / Technologies | Financial Relevance |
|---|---|---|
| **Hardware** | Financial Relevance | Speed, energy efficiency |
| **Algorithms** | Superconducting, trapped ions, photonic | Cryptographic risk and Accelerated Search |
| **Optimization** | Speed, energy efficiency | Routing, scheduling, portfolio and collateral allocation |
| **Machine Learning** | Shor, Grover | Pattern detection, Fraud and Risk Signals |
| **Simulation** | Cryptographic risk and Accelerated Search | Materials modeling |
| **QKD** | QAOA, annealing | High-security links for trading, custody, interbank traffic |

The algorithms domain is closely linked to Q Day, the point when quantum computers can break existing public key cryptography. Shor's algorithm can factor large integers and compute discrete logarithms exponentially faster than classical systems, threatening RSA, ECDSA, and EdDSA schemes that secure blockchain and financial infrastructure.

Q Day should not be seen as a single event but as a continuum of risk realization, unfolding through steady advances in qubit fidelity, error correction, and fault tolerance. Each incremental improvement across these domains increases potential exposure within financial systems.

Most experts project that Q Day level capability could emerge within five to eight years, assuming exponential scaling and stable error correction progress. However, this timeline depends critically on achieving fault tolerant logical qubits, not merely adding more physical qubits or improving benchmark scores such as Quantum Volume. More conservative models extend this horizon into the early to mid-2030s, underscoring both the uncertainty and the urgency of preparing now.

Key Implication: Progress is now driven by qubit quality and error correction rather than just the number of physical qubits. For instance, Google's 105-qubit Willow chip (2024) is considered a major advancement over IBM's 127-qubit Eagle (2021) due to superior quality and error correction.

### Table 2: Quantum Metrics Timeline

**Quantum Computing Benchmarking metrics**

#### 2019–2020: Quantum Volume (QV)

Quantum Volume (QV) combines qubit count, connectivity, fidelity, and circuit depth into one capability score.

#### 2021: QV + CLOPS

CLOPS measures how quickly quantum layers run on hardware, complementing Quantum Volume.

#### 2023: Layer Fidelity + CLOPS_h

Layer Fidelity + CLOPS_h shows how accurately layers of quantum operations execute on real devices.

#### 2024: ECCS + Application Performance + RCS

ECCS +Application Performance + RCS captures error correction cycles per second, application performance, and random circuit sampling.

#### 2025 and beyond: Logical Qubits + Fault Tolerant Throughput

Logical Qubits + Fault Tolerant Throughput shifts focus to error-corrected logical qubits and their fault-tolerant throughput.

## Quantum Risk by Asset Class

Quantum computing poses a material challenge to digital assets by endangering the cryptographic foundations that secure ownership and transaction integrity. The primary vulnerability lies in signature algorithms particularly ECDSA and EdDSA rather than hashing functions such as SHA-256.

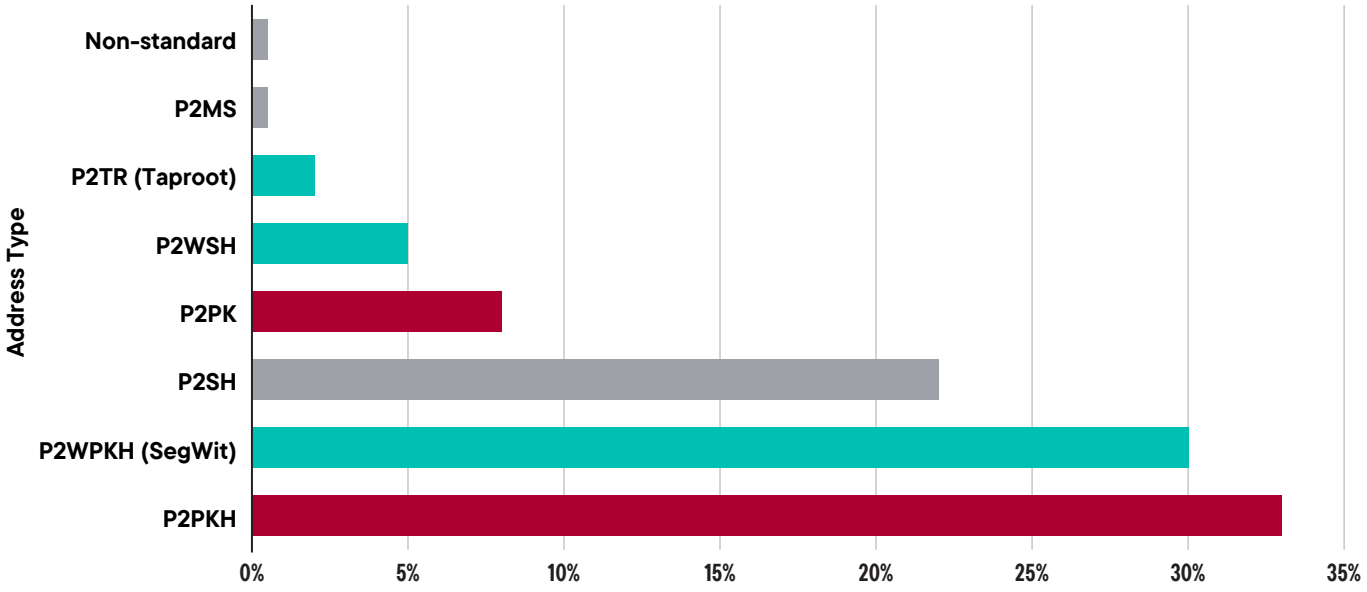
## Table 3: Quantum Risk Across Digital Asset Classes

| Segment / Asset Class | Key Vulnerability | Quantum Exposure Level | Recommended Migration Path |
|---|---|---|---|
| **Bitcoin** | ECDSA signatures vulnerable to Shor's algorithm; SHA-256 hashing largely unaffected | Shown in Fig 1 below | Migrate residual balances to SegWit or Taproot; avoid key reuse; prepare for post-quantum signature upgrades |
| **Smart-Contract Platforms (ETH, SOL, ADA)** | ECDSA/BLS signature schemes at risk once public keys are exposed | Moderate to High | Enable post-quantum signature verification through upgradeable contract frameworks |
| **Stablecoins & DeFi Protocols** | Issuer custody keys, bridges, and smart contracts controlling large funds | Moderate | Introduce hybrid PQC signatures; enforce key rotation and governance redesign |
| **Exchanges & Custodians** | TLS, VPN, and code-signing that rely on classical cryptography | High | Adopt hybrid PQC-TLS (e.g., ML-KEM + X25519); embed crypto-agility into HSM and signing systems |
| **Bridges & Oracles** | Multi-sig or threshold-signature schemes across blockchains | High | Migrate to PQC-enabled threshold schemes; diversify cryptographic dependencies |
| **Layer-2 & Payment Channels** | Channel signatures and withdrawal proofs | Medium | Integrate PQC verification into rollups and state-channel designs |

Bitcoin's exposure depends on address design. Legacy formats (P2PK, P2PKH) that reveal public keys before or during spending are most vulnerable, while SegWit and Taproot conceal public keys until use, offering improved resistance.

**Institutional Implication:** For allocators, exposure concentrates in custody partners and validator infrastructure rather than retail wallet layers.

## Figure1: Bitcoin Supply by Address & Quantum Risk



## Industry Response and Standards Landscape

The quantum threat is now recognized as a strategic risk to global financial and digital-asset infrastructure. A coordinated transition toward post-quantum security is underway across standards bodies, technology providers, and financial institutions.

- **NIST** has standardized **CRYSTALS-Kyber** (encryption) and **CRYSTALS-Dilithium** (signatures). In **March 2025**, it added **Hamming Quasi-Cyclic (HQC)** as a code-based backup to lattice algorithms.
- **NSA** is enforcing the **CNSA 2.0** migration, requiring **ML-KEM** and **SLH-DSA** across U.S. National Security Systems by **2030**, with classical suites phased out after **2025**. The agency warns of the "Harvest Now, Decrypt Later" risk and mandates PQC use for classified systems in its **CSfC Addendum (2025 Draft)**.
- **FS-ISAC** is coordinating **2025–26 hybrid TLS pilots** with **ML-KEM**, publishing PCI quantum-safe guidance and a global roadmap for adoption through **2035**.
- The **IETF PQUIP Working Group** is integrating PQC into **TLS 1.3**, **DNSSEC**, and other Internet protocols, enabling hybrid key exchanges and crypto-agility standards.
- Technology leaders such as **Google, Cloudflare, Akamai, IBM,** and **Keyfactor** have implemented **live hybrid PQC-TLS** and enterprise crypto-lifecycle management tools.
- Financial institutions including **JPMorgan Chase, HSBC** and **Wells Fargo** are testing **Quantum Key Distribution** networks for interbank data protection and transaction security.

## Governance and Upgrade Pathways

Bitcoin's governance model enables technical evolution while preserving decentralization. Upgrades follow the Bitcoin Improvement Proposal (BIP) process—peer review, public testing, and miner signaling—ensuring consensus before activation.

**Post-Quantum BIPs Under Review:**

- BIP-360 (P2QRH, 2024): Introduces hybrid quantum-resistant addresses using FALCON, CRYSTALS-Dilithium, and SPHINCS+.
- Post-Quantum Migration & Legacy Sunset (2025): Proposes phased restrictions on legacy ECDSA addresses and recovery options for exposed funds.
- QRAMP (2025): Outlines wallet migration tooling and exchange readiness for full PQC integration.

**Historical Benchmarks:**

SegWit (2017) and Taproot (2021) upgrades took 2–4 years from proposal to activation. A post-quantum upgrade is expected to follow a 3–5 year timeline, with pilots in 2025–26 and full deployment by 2030, ahead of projected cryptographically relevant quantum computing (CRQC) milestones.

## Institutional Implications:

Custodians, exchanges, and wallet providers should coordinate early on wallet migration schedules, key rotations, and liquidity planning to avoid fragmentation during the PQC transition. Hardware and regulatory pilots such as SEALSQ's PQC-enabled wallets, BTQ's ML-DSA demonstrations, and the SEC PQFIF framework show that governance and infrastructure are already aligning toward a quantum-secure Bitcoin network.

Quantum readiness should now be integrated into operational due diligence (ODD) for digital-asset custodians and funds, aligning with resilience frameworks such as BIS Project Leap and the NSA's CNSA 2.0 guidance. Integrating PQC preparedness into ODD helps ensure that custodians demonstrate not only technical compliance but also proactive risk management and long-term operational resilience.

**Pricing horizon:** We expect partial pricing over the next 12–24 months as PQC-TLS and custody pilots move to production and disclosures improve, with full risk premia differentiation as networks publish BIP-grade migration schedules and begin wallet rotations.

## Strategic Implications of Quantum Transition

The SWOT framework (Figure2: Strategic Implications of the Quantum Transition) highlights how readiness varies across dimensions of policy, technology, and market adoption. Migration to post-quantum security is technically complex, but institutions that move early can set new benchmarks for digital trust and regulatory alignment.

### Strengths

- Global standardization driven by NIST and systemically important infrastructure providers
- Early deployment of hybrid post-quantum cryptography across payment, trading, and custody networks
- Increasing adoption of crypto-agile architectures within institutional technology stacks

### Weaknesses

- High migration costs and operational complexity across legacy and multi-party systems
- Regulatory divergence slowing coordinated industry adoption
- Physical and economic scalability constraints of quantum key distribution

### Opportunities

- First movers capture premium flows in quantum-resilient custody, trading, and settlement
- Creation of new revenue lines through post-quantum security, key-management, and assurance services
- Ability to position “quantum-secure” infrastructure as a fiduciary differentiator and brand advantage

### Threats

- Fragmented or uncoordinated rollouts introducing weak links in cross-border and multi-asset settlement networks
- Accelerated quantum breakthroughs compressing migration windows and triggering confidence or valuation shocks

## Figure 2: Strategic Implications of the Quantum Transition

Institutions that operationalize crypto-agility and align governance with PQC standards now will convert a technical transition into a durable trust advantage.

*Note: Architectural crypto-agility alone does not ensure PQC readiness — operational readiness depends on automated key rotation, certificate renewal, and tested migration pathways.*

*Definition*

**PQ-premium**

**A valuation premium (or lower spread/vol) earned by assets, protocols, and custodians that demonstrate crypto-agility (key inventories, short cert lifetimes, PQC-TLS in production, signed migration plans, testnet PQ-signatures).**

## Conclusion

The advent of quantum computing will not undermine digital assets—but will reorder the hierarchy of trust across the ecosystem. The transition to post-quantum security represents a **strategic modernization of digital infrastructure**, comparable in scale to Y2K remediation or the migration to IPv6, yet with deeper cryptographic and fiduciary consequences.




## For institutional allocators, the implications extend beyond technology:

- **Operational Due Diligence:** Quantum readiness should become a formal criterion in evaluating custodians, token issuers, and blockchain protocols.
- **Valuation and Risk Pricing:** Assets and counterparties demonstrating provable crypto-agility may warrant lower operational risk premia; conversely, legacy exposure could command a discount as migration timelines shorten.
- **Governance and Policy:** Regulators and standards bodies will increasingly view quantum-safe design as integral to operational resilience and investor protection.

The pathway to quantum safety will take years and involve coordinated software upgrades, key rotations, and consensus governance. Historical precedent—SegWit (2017) and Taproot (2021)—suggests that major Bitcoin-level cryptographic transitions require **three to four years** from proposal to activation. A post-quantum upgrade may take longer, underscoring the need to begin preparatory work now, before urgency becomes constraint.

In this light, the firms that lead on crypto agility—those who know every key and certificate they depend on, rotate them without disruption, and maintain test-ready PQC infrastructure—will be the ones that protect client assets, preserve institutional confidence, and earn the premium mandates of the coming decade.

Quantum risk is real, but it is also **actionable**. Institutions that act early can turn a potential systemic vulnerability into a defining source of trust and resilience within the digital asset economy.

References:

1. IBM (2025) IBM Quantum Technology Roadmap. Available at: https://www.ibm.com/quantum/technology#roadmap (Accessed: 30 October 2025).
2. Google Quantum AI (2025) Quantum AI Roadmap. Available at: https://quantumai.google/roadmap (Accessed: 30 October 2025).
3. Google Quantum AI (2024) Willow Spec Sheet. Available at: https://quantumai.google/static/site-assets/downloads/willow-spec-sheet.pdf (Accessed: 30 October 2025).
4. IBM Quantum Blog (2024) Utility Toward Useful Quantum. Available at: https://www.ibm.com/quantum/blog/utility-toward-useful-quantum (Accessed: 30 October 2025).
5. National Security Agency (NSA) (2023) Quantum-Resistant Cryptography: 'Harvest Now, Decrypt Later' Risk. Available at: https://media.defense.gov/2023/Oct/18/2003329018/-1/-1/0/CNSA2.0FACTSHEET.PDF (Accessed: 30 October 2025).
6. National Institute of Standards and Technology (NIST) (2025) Considerations for Achieving Crypto Agility (CSWP 39 Draft). Available at: https://www.nist.gov/news-events/news/2025/03/considerations-achieving-crypto-agility-nist-releases-cswp-39-public (Accessed: 30 October 2025).
7. IBM Quantum Blog (2024) Crypto-Agility for a Post-Quantum World. Available at: https://www.ibm.com/quantum/blog/crypto-agility (Accessed: 30 October 2025).

## WHAT ARE THE RISKS?

**All investments involve risk, including the loss of principal.**

**Digital assets are subject to risks relating to immature and rapidly developing technology,** security vulnerabilities of this technology (such as theft, loss or destruction of cryptographic keys), conflicting intellectual property claims, credit risk of digital asset exchanges, regulatory uncertainty, high volatility in their value/price, unclear acceptance by users and global marketplaces, and manipulation or fraud. Portfolio managers, service providers to the portfolios and other market participants increasingly depend on complex information technology and communications systems to conduct business functions. These systems are subject to a number of different threats or risks that could adversely affect the portfolio and their investors, despite the efforts of the portfolio managers and service providers to adopt technologies, processes and practices intended to mitigate these risks and protect the security of their computer systems, software, networks and other technology assets, as well as the confidentiality, integrity and availability of information belonging to the portfolios and their investors.

Any companies and/or case studies referenced herein are used solely for illustrative purposes; any investment may or may not be currently held by any portfolio advised by Franklin Templeton. The information provided is not a recommendation or individual investment advice for any particular security, strategy or investment product and is not an indication of the trading intent of any Franklin Templeton managed portfolio.

## IMPORTANT LEGAL INFORMATION

This material is intended to be of general interest only and should not be construed as individual investment advice or a recommendation or solicitation to buy, sell or hold any security or to adopt any investment strategy. It does not constitute legal or tax advice. This material may not be reproduced, distributed or published without prior written permission from Franklin Templeton.

The views expressed are those of the investment manager and the comments, opinions and analyses are rendered as at publication date and may change without notice. The underlying assumptions and these views are subject to change based on market and other conditions and may differ from other portfolio managers or of the firm as a whole. The information provided in this material is not intended as a complete analysis of every material fact regarding any country, region or market. There is no assurance that any prediction, projection or forecast on the economy, stock market, bond market or the economic trends of the markets will be realized. The value of investments and the income from them can go down as well as up and you may not get back the full amount that you invested. **Past performance is not necessarily indicative nor a guarantee of future performance.**

Any research and analysis contained in this material has been procured by Franklin Templeton for its own purposes and may be acted upon in that connection and, as such, is provided to you incidentally. Data from third-party sources may have been used in the preparation of this material and Franklin Templeton ("FT") has not independently verified, validated or audited such data. Although information has been obtained from sources that Franklin Templeton believes to be reliable, no guarantee can be given as to its accuracy and such information may be incomplete or condensed and may be subject to change at any time without notice. The mention of any individual securities should neither constitute nor be construed as a recommendation to purchase, hold or sell any securities, and the information provided regarding such individual securities (if any) is not a sufficient basis upon which to make an investment decision. FT accepts no liability whatsoever for any loss arising from use of this information and reliance upon the comments, opinions and analyses in the material is at the sole discretion of the user.

Products, services and information may not be available in all jurisdictions and are offered outside the US by other Franklin Templeton affiliates and/or their distributors as local laws and regulation permits. Please consult your own financial professional or Franklin Templeton institutional contact for further information on availability of products and services in your jurisdiction.

**Brazil:** Issued by Franklin Templeton Investimentos (Brasil) Ltda., authorized to render investment management services by CVM per Declaratory Act n. 6.534, issued on October 1, 2001.

**Canada:** Issued by Franklin Templeton Investments Corp., 200 King Street West, Suite 1500 Toronto, ON, M5H3T4, Fax: (416) 364-1163, (800) 387-0830, www.franklintempleton.ca. **Offshore Americas:** In the US, this publication is made available by Franklin Templeton, One Franklin Parkway, San Mateo, California 94403-1906. Tel: (800) 239-3894 (USA Toll-Free), (877) 389-0076 (Canada Toll-Free), and Fax: (727) 299-8736. US: by Franklin Templeton, One Franklin Parkway, San Mateo, California 94403-1906, (800) DIAL BEN/342-5236, www.franklintempleton.com. Investments are not FDIC insured; may lose value; and are not bank guaranteed.

Issued in **Europe** by: Franklin Templeton International Services S.à r.l.—Supervised by the Commission de Surveillance du Secteur Financier–8A, rue Albert Borschette, L-1246 Luxembourg. Tel: +352-46 66 67-1, Fax: +352-46 66 76. **Poland:** Issued by Templeton Asset Management (Poland) TFI S.A.; Rondo ONZ 1; 00-124 Warsaw. **South Africa:** Issued by Franklin Templeton Investments SA (PTY) Ltd, which is an authorised Financial Services Provider. Tel: +27 (21) 831 7400, Fax: +27 (21) 831 7422. **Switzerland:** Issued by Franklin Templeton Switzerland Ltd, Stockerstrasse 38, CH-8002 Zurich. **United Arab Emirates:** Issued by Franklin Templeton Investments (ME) Limited, authorized and regulated by the Dubai Financial Services Authority. Dubai office: Franklin Templeton, The Gate, East Wing, Level 2, Dubai International Financial Centre, P.O. Box 506613, Dubai, U.A.E. Tel: +9714-4284100, Fax: +9714-4284140. **UK:** Issued by Franklin Templeton Investment Management Limited (FTIML), registered office: Cannon Place, 78 Cannon Street, London EC4N 6HL. Tel: +44 (0)20 7073 8500. Authorized and regulated in the United Kingdom by the Financial Conduct Authority. **Saudi Arabia:** Franklin Templeton Financial Company, Unit 209, Rubeen Plaza, Northern Ring Rd, Hittin District 13512, Riyadh, Saudi Arabia. Regulated by CMA. License no. 23265-22. Tel: +966-112542570. All investments entail risks including loss of principal investment amount.

**Australia:** Issued by Franklin Templeton Australia Limited (ABN 76 004 835 849) (Australian Financial Services License Holder No. 240827), Level 47, 120 Collins Street, Melbourne, Victoria 3000. **Hong Kong:** Issued by Franklin Templeton Investments (Asia) Limited, 62/F, Two IFC, 8 Finance Street, Central, Hong Kong. **Japan:** Issued by Franklin Templeton Investments Japan Limited. **Korea:** Franklin Templeton Investment Advisors Korea Co., Ltd., 3rd fl., CCMM Building, 101 Yeouigongwon-ro, Yeongdeungpo-gu, Seoul, Korea 07241. **Malaysia:** Issued by Franklin Templeton Asset Management (Malaysia) Sdn. Bhd. & Franklin Templeton GSC Asset Management Sdn. Bhd. This document has not been reviewed by Securities Commission Malaysia. **Singapore:** Issued by Templeton Asset Management Ltd. Registration No. (UEN) 199205211E, 7 Temasek Boulevard, #38-03 Suntec Tower One, 038987, Singapore.

Please visit www.franklinresources.com to be directed to your local Franklin Templeton website.

---



FRANKLIN TEMPLETON

**franklintempleton.com**

© 2025 Franklin Distributors, LLC. Member FINRA/SIPC. All rights reserved.

US-RETM-8234758-8134758
DASQE-FL-0126

FRANKLIN TEMPLETON

Perspective from Franklin Templeton Digital Assets

# Technical appendix: Quantum threat demystified

November 2025 | White Paper


## Abstract

This appendix provides the technical foundation and source validation for the Franklin Templeton paper, Digital Asset Security in the Quantum Era.

It expands on the key concepts, data, and references underpinning the investment-oriented analysis, offering deeper detail for readers who wish to understand the underlying quantum computing landscape, cryptographic dependencies, and the transition toward post-quantum security.

Where the flagship paper focuses on strategic implications for institutional allocators, this appendix addresses the engineering and governance realities that make those conclusions credible.

It includes quantitative benchmarks, taxonomy tables, and references to the leading academic, industrial, and regulatory initiatives shaping the post-quantum transition.

The intended audience includes:

- Institutional technology and operations teams supporting custody and trading infrastructure.
- Due diligence professionals evaluating digital asset risk frameworks.

Regulators, consultants, and counterparties requiring validated technical sourcing.

The appendix should be read as **supporting documentation**, not a standalone publication. It provides technical depth and citations that enable allocators to confidently reference or audit the underlying assumptions presented in the main paper.


## Section 1–Quantum Computing Fundamentals (Condensed Overview)

Quantum computing applies the principles of quantum mechanics to process information beyond the limits of classical computation. Instead of using bits that represent either 0 or 1, quantum computers use qubits or quantum bits. A qubit can exist in a combination of both 0 and 1 at once due to a property known as superposition. When multiple qubits interact, they can also become entangled, meaning the state of one qubit is linked to the state of another even when they are far apart.

The field of quantum computing is best viewed through six research domains as shown in the following table: *Quantum Computing Research Domains*

### Table 1: Quantum Computing Research Domains

| **Domain** | Example Algorithms / Technologies | Financial Relevance |
|---|---|---|
| **Hardware** | Financial Relevance | Speed, energy efficiency |
| **Algorithms** | Superconducting, trapped ions, photonic | Cryptographic risk and Accelerated Search |
| **Optimization** | Speed, energy efficiency | Routing, scheduling, portfolio and collateral allocation |
| **Machine Learning** | Shor, Grover | Pattern detection, Fraud and Risk Signals |
| **Simulation** | Cryptographic risk and Accelerated Search | Materials modeling |
| **QKD** | QAOA, annealing | High-security links for trading, custody, interbank traffic |


Not FDIC Insured | No Bank Guarantee | May Lose Value

The Algorithms domain in quantum computing is directly tied to the concept of **Q-Day**, when a quantum computer can break today's public-key cryptography. Shor's algorithm can factor large integers and compute discrete logarithms exponentially faster than classical systems, compromising RSA, ECDSA, and EdDSA schemes that secure blockchain and financial infrastructure.

Most experts estimate Q-Day to arrive within the **next five to eight years** as illustrated in the timeline below. This makes algorithmic research not just theoretical but a countdown to when cryptographic transition becomes urgent. For institutional allocators and financial networks, Q-Day represents a systemic risk inflection point, where proactive migration to post-quantum cryptography (PQC) determines operational resilience and market trust.

**Quantum Computing Milestones**
1980–2033+

**1980** Benioff proposes a quantum Turing machine

**1981** Feynman argues for simulating physics wth quantum computers

**1985** Deutsch defines a universal quantum computer

**1994** Shor publishes polynomial-time & discrete-log quantum algorithms

**1998** First experimental demos of quantum algorithms on 2–3-qubit NMR devices

**2001** Shor's algorith demo: factoring 15 with a 7-qubit NMR system

**2016** IBM Quantum Experience launches (5 qubits)–first cloud quantum computer

**2019** Google Sycamore (53 qubits) claims quantum supremacy

**2021** IBM unvels Eagle (127-qubits superconducting processor)

**2023** IBM debuts Heron (133 qubits) & Quantum System Two

**2024** Google's Willow (105 qubits)

**2025** IBM Nighthawk: ~5K gates, 120 qubits (error-mitigated)

**2026** IBM targets first examples of quantum advantage (~100M gates, 120 qubits)

**2029** IBM Starling: ~200 logical qubits & ~100M logical gates (fault tolerent)

**2033** IBM Roadmaps anticipate ~2,000 logical qubits and billion-gate circuits

**As represented in the timeline, while IBM's Eagle processor (2021) has more qubits (127) than Google's Willow chip (2024) (105), Willow is regarded as a major advancement because it excels in qubit quality and error correction, which are arguably more important than sheer qubit count at this stage of quantum computing. Consequently, we can't directly compare quantum computing progress to Moore's Law.**

## Section 2–Measuring Quantum Progress: Quality over Count

Measuring quantum performance goes beyond counting qubits. Over time, benchmarking has evolved from focusing on raw qubit numbers to assessing logical qubits and error-correction efficiency, which define when cryptographically relevant computation becomes feasible. For example, although Google's Willow processor launched in 2024 with 105 physical qubits, it outperforms IBM's Eagle processor from 2021 with 127 physical qubits because it achieves higher qubit quality, better connectivity, and improved error correction, factors that are increasingly more important than qubit count alone.

### Table 2: Quantum Metrics Timeline

**Quantum Computing Benchmarking metrics**

#### 2019–2020: Quantum Volume (QV)

Quantum Volume (QV) combines qubit count, connectivity, fidelity, and circuit depth into one capability score.

#### 2021: QV + CLOPS

CLOPS measures how quickly quantum layers run on hardware, complementing Quantum Volume.

#### 2023: Layer Fidelity + CLOPS_h

Layer Fidelity + CLOPS_h shows how accurately layers of quantum operations execute on real devices.

#### 2024: ECCS + Application Performance + RCS

ECCS +Application Performance + RCS captures error correction cycles per second, application performance, and random circuit sampling.

#### 2025 and beyond: Logical Qubits + Fault Tolerant Throughput

Logical Qubits + Fault Tolerant Throughput shifts focus to error-corrected logical qubits and their fault-tolerant throughput.

*Note: Physical Qubit → Error-Detection → Error-Correction → Fault-Tolerant Logical Qubit*

Institutional Implication: Hardware maturity is now measured in "error-corrected logical qubits," which define when cryptographically relevant computation becomes feasible. QV and CLOPS increases do not directly equate to cryptographic threat maturity.

## Section 3–Timeline to Cryptographic Relevance

No quantum computer today is capable of executing Shor's algorithm at the scale required to break RSA-2048 or elliptic curve keys (ECDSA/EdDSA). Current estimates place such capability well beyond existing hardware.

**Key Milestones and Estimates**

- 2019 (Gidney & Ekerå): Estimated ~20 million physical qubits needed to factor RSA-2048 in eight hours under surface-code assumptions.
- 2024 (Google Willow): Demonstrated below-threshold error correction across 3×3 → 5×5 → 7×7 qubit arrays, marking the first clear step toward fault tolerance.
- 2025 (Updated Gidney Model): Reduced the requirement to under one million noisy qubits by introducing approximate arithmetic and optimized error handling, though still under idealized hardware conditions.
- 2029 (IBM Starling Roadmap): Targets ~200 logical qubits capable of executing 100 million-gate circuits—potentially the first generation of fault-tolerant prototypes.

*Interpretive Note:*
Timelines depend primarily on progress in fault-tolerant logical qubits rather than physical qubit count. Most forecasts now place potential cryptographic relevance between the late 2020s and mid-2030s, depending on how rapidly coherence, error correction, and scaling advance.

### Figure 1: Quantum Hardware Maturity and Cryptographic Risk Horizon

**2024**
- Below-threshold error correction achieved (Google *Willow* processor)
- First proof that logical error rates decline with increasing qubit array size

**2025–2029**
- Fault-tolerant prototype era begins
- IBM *Starling* roadmap targets ~200 logical qubits
- Experimental ciruits reach 100M–gate scale

**2030+**
- Emergence of cryptographically relevant quantum systems
- Potential threat to RSA-2048/ECDSA security
- Migration to Post-Quantum Crypotgraphy (PQC) critical

## Section 4–Quantum Risk by Asset Class (Core Value Add)

Quantum computing introduces varying degrees of exposure across digital assets, driven by signature visibility, key management practices, and protocol upgradeability. Table 3: Evolution of Bitcoin Address Types and Figure: Bitcoin Supply by Address and Quantum Risk together illustrate that signature exposure—rather than hashing—is the primary determinant of vulnerability.

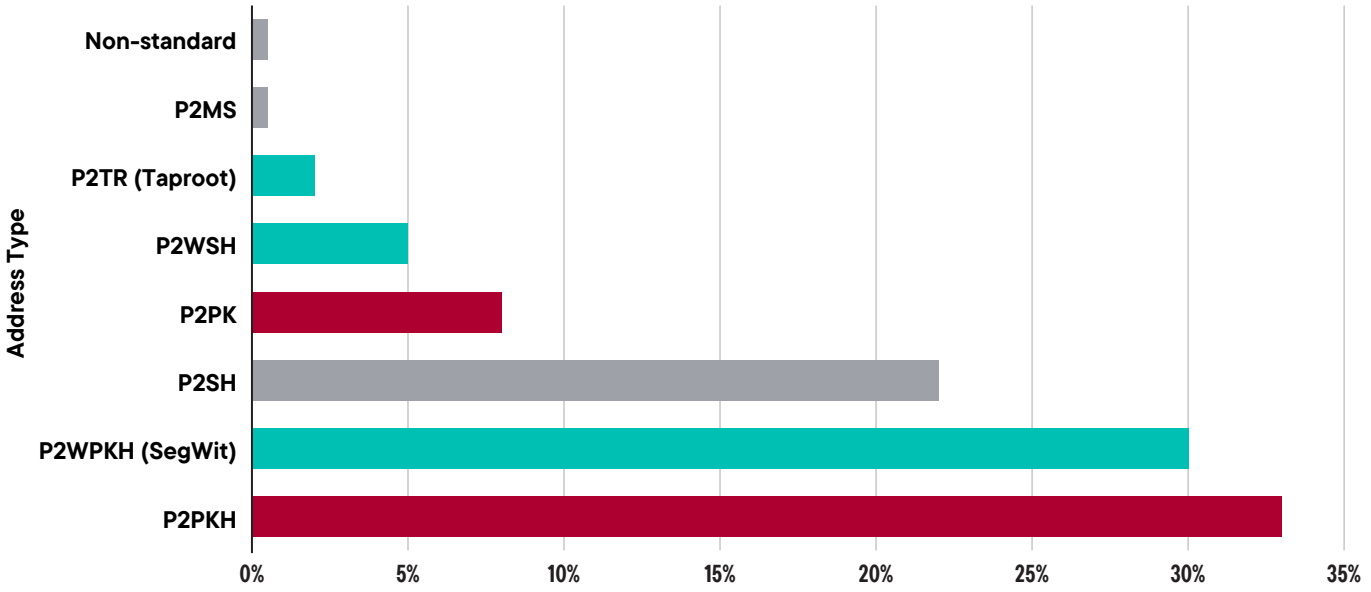
- Bitcoin: ECDSA is the weak link. Legacy outputs that reveal public keys before or at spend carry the highest exposure. Residual balances should be migrated to SegWit or Taproot, key reuse should be avoided, and preparations should begin for post-quantum signature upgrades.
- Smart-contract platforms (ETH, SOL, ADA): User and validator keys on ECDSA or EdDSA are vulnerable once public keys are exposed. Account abstraction and upgradeable contracts enable a shift to post-quantum verification.
- Stablecoins and tokenized assets: Risk centers on issuer custody keys and mint–burn controls. Upgradeable contracts allow controlled migration and key rotation.
- DeFi, bridges, oracles: Multisig and threshold schemes on classical curves create concentrated points of failure. Governance and bridge validation should be redesigned for crypto-agility.

- Custodians, exchanges, wallets: Exposure extends to TLS, VPNs, code-signing, and HSM policies. Adopting hybrid PQC-TLS and shortening certificate and key lifetimes enhance resilience.
- Layer-2 systems: Channels and rollups rely on classical signatures for state and exits. Short timelocks help, but durable protection requires PQC-capable channel and rollup logic.

## Table 3: Evolution of Bitcoin address types and purpose

| Address Type | Year Introduced | Purpose & Key Feature | Reason for Exposure |
|---|---|---|---|
| **P2PK (Pay-to-Public-Key)** | 2009 | Original format used by early Bitcoin transactions. Public keys are exposed, offering little privacy or protection. | Full public key appears directly on-chain, making private key recovery possible with Shor's algorithm. |
| **P2PKH (Pay-to-Public-Key-Hash)** | 2009 | Added hashing to public keys for better security and smaller transactions. It became the dominant format in early wallets. | The public key is hidden until spent but becomes visible post-transaction, leaving residual exposure. |
| **P2SH (Pay-to-Script-Hash)** | 2012 | Enabled complex scripts and multi-signature wallets by storing only the script hash on-chain. | Multisig and script hashing improve privacy; keys are revealed only at spend. |
| **P2WPKH (Pay-to-Witness-Public-Key-Hash)** | 2017 | Part of SegWit upgrade; reduced transaction fees and fixed malleability issues. Public keys remain hidden until use. | SegWit reduces fees and hides keys until use, minimizing on-chain exposure. |
| **P2WSH (Pay-to-Witness-Script-Hash)** | 2017 | SegWit version of P2SH supporting advanced scripts with better efficiency and privacy. | Offers enhanced privacy; keys remain concealed until execution, lowering exposure risk. |
| **P2MS (Pay-to-Multi-Sig)** | 2017 | Allowed multiple keys to control one wallet, offering shared custody but exposing public keys. | Public keys for all signers are revealed, creating multiple points of exposure to quantum attacks. |
| **P2TR (Pay-to-Taproot)** | 2021 | Latest upgrade using Schnorr signatures and Merkle trees for privacy, scalability, and quantum resistance. | Keys are aggregated and hidden until necessary, offering the strongest privacy and lowest quantum exposure among address types. |

## Figure2: Bitcoin Supply by Address & Quantum Risk




*Institutional Implication: For allocators, exposure concentrates in custody partners and validator infrastructure rather than retail wallet layers.*

## Section 5–Industry Response and Standards Landscape

The quantum threat is increasingly recognized as a strategic risk to financial infrastructure and digital-asset custody systems. Across standards bodies, technology providers, and major financial institutions, a coordinated effort is underway to transition toward post-quantum security.

### 1. Standards and Regulatory Bodies

**NIST (National Institute of Standards and Technology):** NIST leads the global effort to standardize post-quantum cryptography through CRYSTALS Kyber for key exchange and CRYSTALS Dilithium for digital signatures. In March 2025, NIST selected Hamming Quasi-Cyclic (HQC) as the fifth post-quantum algorithm for standardization. HQC is a code-based key encapsulation mechanism that complements ML-KEM by providing diversification against potential lattice-based vulnerabilities.

**NSA (National Security Agency):** The NSA leads U.S. government efforts to secure National Security Systems (NSS) against quantum threats, overseeing the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) to mandate quantum-resistant algorithms. In 2025, it updated CNSSP 15 to enforce adoption of ML-KEM for encryption and SLH-DSA for digital signatures, requiring vendors to prefer these by the end of 2025, with exclusive use by 2030 and full NSS compliance by 2033. The NSA highlights the "Harvest Now, Decrypt Later" (HNDL) risk, urging immediate transition planning to protect long-lived classified data. Its CSfC Post-Quantum Guidance Addendum (Draft 2025) specifies that CNSA 1.0 algorithms are valid only until December 31, 2025, after which CNSA 2.0 becomes mandatory for classified data protection, with hybrid modes allowed as temporary transition options. This aligns with the broader goal of achieving quantum resistance across NSS by 2035, as outlined in National Security Memorandum 10 (NSM-10).

**FS-ISAC (Financial Services Information Sharing and Analysis Center):** FS-ISAC's PQC Working Group (WG) is coordinating 2025–26 hybrid TLS pilots in payment networks (e.g., ML-KEM tests post-PCI inventories) and urging immediate crypto asset mapping to counter Harvest Now risks across 20B+ devices.

**Key achievements:**

- Feb 2025: PCI Guidance – 4 papers (1 leader guide + 3 use cases: provisioning, routing, POS) for quantum-safe card data.
- Sep 2025: Migration Timeline WP – Global roadmap to 2035 adoption, led by Peter Bordow (Wells Fargo).

**IETF (Internet Engineering Task Force):**

- The IETF's PQUIP WG, launched January 2025, is driving post-quantum (PQC) integration across internet protocols, focusing on hybrid modes (e.g., X25519 + ML-KEM-768), TLS 1.3 enhancements, and migration use cases to ensure resilience.
- So far, they've adopted a March 2025 hybrid key exchange draft for TLS, released an August 2025 engineer guide (v14) on crypto-agility, and advanced September–October 2025 drafts for constrained devices and DNSSEC, tracked via their GitHub repo.
- They also hosted the IETF 122 Hackathon (September 2025) to embed PQC in tools like Nmap, with support from Microsoft and Akamai for TLS 1.3 hybrids.

### 2. Technology and Infrastructure Providers

**Google, Cloudflare, Akamai:**

- Cloudflare: >50% of traffic now uses hybrid PQC-TLS (X25519 + ML-KEM); mid-Sep 2025 auto-upgraded 6M domains; Zero Trust protects any protocol by mid-2025.
- Akamai: Edge PQC live; Jun 30, 2025 origin support; Sep 1, 2025 browser-to-edge; General Availability Oct 31, 2025; full network Q4 2025–Q1 2026.
- Google: Hybrid ALTS/TLS internal; pioneered CECPQ2 experiments; preps Chrome for ML-KEM.
- Tools: Cloudflare Automatic SSL/TLS, Akamai Ghost-to-Origin for API/wallet/exchange security.




**IBM:**

- Quantum Safe Suite: Discover/Observe/Transform via Explorer/Advisor/Remediator; CBOM generation; Guardium Cryptography Manager (Nov 2025) for AI-driven lifecycle.
- Crypto-agility roadmaps: No-disruption swaps; z16 hardware supports SLH-DSA; aligns NSA 2025 prefs.

**Keyfactor:**

- Command 25.1 (Apr 2025): Inventories ALL PQC certs (ML-DSA, OIDs); hybrid RSA/ML-DSA issuance.
- EJBCA 9.3: HSM + SLH-DSA; PQC Lab (free sandbox); shortens lifetimes via automation/rotation.

**Financial Institutions and Custodians**

- HSBC, JPMorgan Chase, Wells Fargo:
  - JPMorgan: QKD network w/ Toshiba/Ciena (2022–2025); 800Gbps blockchain-secure; Q-CAN (2024) for multi-VPNs.
  - HSBC: BT/Toshiba QSMN (2023); first bank on quantum-secure metro; Quantinuum randomness for gold tokens.
  - Wells Fargo: QKD symmetric keys w/ Toshiba/Ciena (2024); interbank/data-center secure.
  - Pilots: Interbank channels via QKD (quantum + fiber).
- Custody Platforms (Coinbase Custody, Fireblocks, Anchorage Digital):
  - Coinbase Custody: Testing hybrid PQC stacks (e.g., ML-KEM + classical) with MPC and cold staking as an FS-ISAC member.
  - Securing regulated NY trust assets and ensuring SOC audit compliance against quantum risks.
  - Pilots align with FS-ISAC PQC Hub for 2025–26 testing.
- Fireblocks:
  - Deploying MPC stacks with policy-driven key rotation and hybrid PQC (e.g., ML-DSA).
  - Protecting >500+ assets in DeFi/transfers as a BSSC founder.
  - Supports FS-ISAC's 2026–29 phase with NIST standards (FIPS 203, 205).

**Anchorage Digital:**

- Integrating hybrid PQC (e.g., SLH-DSA) with bank-grade HSMs and biometrics in Porto self-custody.
- Safeguarding Fed-chartered/DoJ assets for regulatory compliance.
- Prepares for 2030 PQC default per NIST PQC standards.

## Section 6 – Governance and Upgrade Pathways

Bitcoin's governance model allows evolution while maintaining decentralization. Network upgrades begin as Bitcoin Improvement Proposals (BIPs), which outline new features or cryptographic standards. For post-quantum readiness, several key BIPs are already under review.

Active and Proposed BIPs for PQC:

- BIP-360 (Pay-to-Quantum-Resistant-Hash, P2QRH, June 2024): Introduces hybrid signature addresses (bc1r) combining ECC and PQC algorithms such as FALCON, CRYSTALS-Dilithium, and SPHINCS+. Updated in Feb 2025 with test vectors and soft-fork compatibility.
- Post-Quantum Migration & Legacy Sunset BIP (Lopp et al., July 2025): Phased soft-fork plan to restrict sends to vulnerable addresses (Phase A), freeze ECDSA/Schnorr usage (Phase B ≈ 2 years later), and enable legacy recovery via BIP-39 proofs (Phase C). Targets ≈ 25% of exposed BTC (~$500 B).
- QRAMP BIP (Cruz, Apr 2025): Hard-fork proposal mandating full wallet migration to PQC with exchange and custody tooling.

These proposals follow Bitcoin's standard governance cycle of peer review, public discussion on developer forums, testnet trials, and miner signaling before activation. Soft forks remain the preferred method for maintaining backward compatibility.

| Upgrade | Proposal | Activation | Duration |
|---|---|---|---|
| **SegWit (BIP-141)** | 2015 | August 2017 | About 2 years |
| **Taproot (BIPs 340–342)** | January 2018 | November 2021 | About 4 years |

A post-quantum upgrade is expected to take about three to five years, with pilot phases likely between 2025 and 2026 and full migration before 2030, ahead of projected cryptographically relevant quantum computing (CRQC) timelines around 2027 to 2030.

**Institutional Implications:**

Custodians, exchanges, and wallet providers should coordinate early on wallet migration schedules, key rotations, and liquidity planning to prevent fragmentation during the PQC transition. Hardware and regulatory pilots already demonstrate readiness: the SEALSQ QS7001 (May 2025) introduces PQC hardware for Bitcoin cold wallets, BTQ's ML-DSA demonstration (October 2025) replaces ECDSA with post-quantum signatures, and the SEC PQFIF framework (September 2025) mandates hybrid migration for exchanges and custodians by 2035. These coordinated efforts show that governance, infrastructure, and financial systems are moving together toward a quantum-secure Bitcoin network.

## Section 7–Strategic Implications and SWOT Recap

The quantum transition is not a single disruptive event but an extended operational and regulatory migration requiring sustained coordination. It requires coordinated upgrades across custody systems, validator infrastructure, and network governance frameworks. For financial institutions, this shift represents both a risk exposure and a strategic opportunity.

The SWOT framework (Figure3: Strategic Implications of the Quantum Transition) highlights how readiness varies across dimensions of policy, technology, and market adoption. Migration to post-quantum security is technically complex, but institutions that move early can set new benchmarks for digital trust and regulatory alignment.

**Key Insights:**

- Migration is as much an operational and governance challenge as a cryptographic one.
- Regulatory divergence across jurisdictions increases coordination risk, emphasizing the need for early standard alignment.
- First movers in adopting post-quantum standards can strengthen market confidence and attract long-term institutional flows.

Institutions that operationalize crypto-agility and align governance with post-quantum standards now will convert a technical transition into a durable trust advantage which are preserving asset integrity and investor confidence as the quantum era unfolds.

### Figure 3: Strategic Implications of the Quantum Transition

**Strengths**

- Global standardization driven by NIST and systemically important infrastructure providers
- Early deployment of hybrid post-quantum cryptography across payment, trading, and custody networks
- Increasing adoption of crypto-agile architectures within institutional technology stacks

**Weaknesses**

- High migration costs and operational complexity across legacy and multi-party systems
- Regulatory divergence slowing coordinated industry adoption
- Physical and economic scalability constraints of quantum key distribution

**Opportunities**

- First movers capture premium flows in quantum-resilient custody, trading, and settlement
- Creation of new revenue lines through post-quantum security, key-management, and assurance services
- Ability to position “quantum-secure” infrastructure as a fiduciary differentiator and brand advantage

**Threats**

- Fragmented or uncoordinated rollouts introducing weak links in cross-border and multi-asset settlement networks
- Accelerated quantum breakthroughs compressing migration windows and triggering confidence or valuation shocks

## References


**A. Cryptographic Resource Estimates**

IBM Quantum (2025) IBM Quantum Technology Roadmap. Available at: https://www.ibm.com/quantum/technology#roadmap (Accessed: 29 October 2025).

Google Quantum AI (2025) Google Quantum AI Roadmap. Available at: https://quantumai.google/roadmap (Accessed: 29 October 2025).

Shor, P.W. (1994) 'Algorithms for quantum computation: discrete logarithms and factoring', Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, pp. 124–134. doi: 10.1109/SFCS.1994.365700.

Yoder, T.J., Schoute, E., Rall, P., Pritchett, E., Gambetta, J.M., Cross, A.W., Carroll, M. and Beverland, M.E. (2025) Tour de gross: A modular quantum computer based on bivariate bicycle codes. arXiv preprint arXiv:2506.03094.

IBM Quantum Blog (2021) 127-Qubit Quantum Processor Eagle. Available at: https://www.ibm.com/quantum/blog/127-qubit-quantum-processor-eagle (Accessed: 29 October 2025).

**B. Quantum Hardware & Benchmarks**

Google Quantum AI (2024) Willow Spec Sheet. Available at: https://quantumai.google/static/site-assets/downloads/willow-spec-sheet.pdf (Accessed: 29 October 2025).

IBM Quantum Blog (2025) Utility Toward Useful Quantum. Available at: https://www.ibm.com/quantum/blog/utility-toward-useful-quantum (Accessed: 29 October 2025).

Medium (2023) What Is Quantum Volume Anyway? Available at: https://medium.com/qiskit/what-is-quantum-volume-anyway-a4dff801c36f (Accessed: 29 October 2025).

**C. Bitcoin Supply by Address & Quantum Risk**

Mempool Space (2025) UTXO Set Report, 14 April.

Unchained (2023) Bitcoin Address Types Compared: P2PKH, P2SH, P2WPKH, and More, 2 August.

Bitcoin Magazine (2025) P2PKH, P2SH, P2WPKH, and More, 27 September.

Chainalysis Blog (2025) Mapping the Universe of 460 Million Bitcoin Addresses, 22 June.

Unchained (2018) Bitcoin Data Science (Pt. 3): Dust & Thermodynamics, 17 December.

Hiro Systems (2024) Understanding the Differences Between Bitcoin Address Formats When Developing Your App, 22 August.

Supra (2021) Bitcoin Taproot Update: Compelling or Inconsequential?, 9 December.

Navarro, G. et al. (2019) 'Analysis of the Bitcoin UTXO Set', Financial Cryptography.

Blockchain.com (2024) Blockchain Charts – Total Circulating Bitcoin, 27 October.

**WHAT ARE THE RISKS?**
**All investments involve risk, including the loss of principal.**

**Digital assets are subject to risks relating to immature and rapidly developing technology, security vulnerabilities of this technology** (such as theft, loss or destruction of cryptographic keys), conflicting intellectual property claims, credit risk of digital asset exchanges, regulatory uncertainty, high volatility in their value/price, unclear acceptance by users and global marketplaces, and manipulation or fraud. Portfolio managers, service providers to the portfolios and other market participants increasingly depend on complex information technology and communications systems to conduct business functions. These systems are subject to a number of different threats or risks that could adversely affect the portfolio and their investors, despite the efforts of the portfolio managers and service providers to adopt technologies, processes and practices intended to mitigate these risks and protect the security of their computer systems, software, networks and other technology assets, as well as the confidentiality, integrity and availability of information belonging to the portfolios and their investors.

Any companies and/or case studies referenced herein are used solely for illustrative purposes; any investment may or may not be currently held by any portfolio advised by Franklin Templeton. The information provided is not a recommendation or individual investment advice for any particular security, strategy or investment product and is not an indication of the trading intent of any Franklin Templeton managed portfolio.

**IMPORTANT LEGAL INFORMATION**
This material is intended to be of general interest only and should not be construed as individual investment advice or a recommendation or solicitation to buy, sell or hold any security or to adopt any investment strategy. It does not constitute legal or tax advice. This material may not be reproduced, distributed or published without prior written permission from Franklin Templeton.

The views expressed are those of the investment manager and the comments, opinions and analyses are rendered as at publication date and may change without notice. The underlying assumptions and these views are subject to change based on market and other conditions and may differ from other portfolio managers or of the firm as a whole. The information provided in this material is not intended as a complete analysis of every material fact regarding any country, region or market. There is no assurance that any prediction, projection or forecast on the economy, stock market, bond market or the economic trends of the markets will be realized. The value of investments and the income from them can go down as well as up and you may not get back the full amount that you invested. **Past performance is not necessarily indicative nor a guarantee of future performance.**

Any research and analysis contained in this material has been procured by Franklin Templeton for its own purposes and may be acted upon in that connection and, as such, is provided to you incidentally. Data from third-party sources may have been used in the preparation of this material and Franklin Templeton ("FT") has not independently verified, validated or audited such data. Although information has been obtained from sources that Franklin Templeton believes to be reliable, no guarantee can be given as to its accuracy and such information may be incomplete or condensed and may be subject to change at any time without notice. The mention of any individual securities should neither constitute nor be construed as a recommendation to purchase, hold or sell any securities, and the information provided regarding such individual securities (if any) is not a sufficient basis upon which to make an investment decision. FT accepts no liability whatsoever for any loss arising from use of this information and reliance upon the comments, opinions and analyses in the material is at the sole discretion of the user.

Products, services and information may not be available in all jurisdictions and are offered outside the US by other Franklin Templeton affiliates and/or their distributors as local laws and regulation permits. Please consult your own financial professional or Franklin Templeton institutional contact for further information on availability of products and services in your jurisdiction.

**Brazil:** Issued by Franklin Templeton Investimentos (Brasil) Ltda., authorized to render investment management services by CVM per Declaratory Act n. 6.534, issued on October 1, 2001.

**Canada:** Issued by Franklin Templeton Investments Corp., 200 King Street West, Suite 1500 Toronto, ON, M5H3T4, Fax: (416) 364-1163, (800) 387-0830, www.franklintempleton.ca. **Offshore Americas:** In the US, this publication is made available by Franklin Templeton, One Franklin Parkway, San Mateo, California 94403-1906. Tel: (800) 239-3894 (USA Toll-Free), (877) 389-0076 (Canada Toll-Free), and Fax: (727) 299-8736. US: by Franklin Templeton, One Franklin Parkway, San Mateo, California 94403-1906, (800) DIAL BEN/342-5236, www.franklintempleton.com. Investments are not FDIC insured; may lose value; and are not bank guaranteed.

Issued in **Europe** by: Franklin Templeton International Services S.à r.l.—Supervised by the Commission de Surveillance du Secteur Financier–8A, rue Albert Borschette, L-1246 Luxembourg. Tel: +352-46 66 67-1, Fax: +352-46 66 76. **Poland:** Issued by Templeton Asset Management (Poland) TFI S.A.; Rondo ONZ 1; 00-124 Warsaw. **South Africa:** Issued by Franklin Templeton Investments SA (PTY) Ltd, which is an authorised Financial Services Provider. Tel: +27 (21) 831 7400, Fax: +27 (21) 831 7422. **Switzerland:** Issued by Franklin Templeton Switzerland Ltd, Stockerstrasse 38, CH-8002 Zurich. **United Arab Emirates:** Issued by Franklin Templeton Investments (ME) Limited, authorized and regulated by the Dubai Financial Services Authority. Dubai office: Franklin Templeton, The Gate, East Wing, Level 2, Dubai International Financial Centre, P.O. Box 506613, Dubai, U.A.E. Tel: +9714-4284100, Fax: +9714-4284140. **UK:** Issued by Franklin Templeton Investment Management Limited (FTIML), registered office: Cannon Place, 78 Cannon Street, London EC4N 6HL. Tel: +44 (0)20 7073 8500. Authorized and regulated in the United Kingdom by the Financial Conduct Authority. **Saudi Arabia:** Franklin Templeton Financial Company, Unit 209, Rubeen Plaza, Northern Ring Rd, Hittin District 13512, Riyadh, Saudi Arabia. Regulated by CMA. License no. 23265-22. Tel: +966-112542570. All investments entail risks including loss of principal investment amount.

**Australia:** Issued by Franklin Templeton Australia Limited (ABN 76 004 835 849) (Australian Financial Services License Holder No. 240827), Level 47, 120 Collins Street, Melbourne, Victoria 3000. **Hong Kong:** Issued by Franklin Templeton Investments (Asia) Limited, 62/F, Two IFC, 8 Finance Street, Central, Hong Kong. **Japan:** Issued by Franklin Templeton Investments Japan Limited. **Korea:** Franklin Templeton Investment Advisors Korea Co., Ltd., 3rd fl., CCMM Building, 101 Yeouigongwon-ro, Yeongdeungpo-gu, Seoul, Korea 07241. **Malaysia:** Issued by Franklin Templeton Asset Management (Malaysia) Sdn. Bhd. & Franklin Templeton GSC Asset Management Sdn. Bhd. This document has not been reviewed by Securities Commission Malaysia. **Singapore:** Issued by Templeton Asset Management Ltd. Registration No. (UEN) 199205211E, 7 Temasek Boulevard, #38-03 Suntec Tower One, 038987, Singapore.

Please visit www.franklinresources.com to be directed to your local Franklin Templeton website.



FRANKLIN TEMPLETON

**franklintempleton.com**

© 2025 Franklin Distributors, LLC. Member FINRA/SIPC. All rights reserved.

US-RETM-8234758-8134758
DASQE-FL-0126