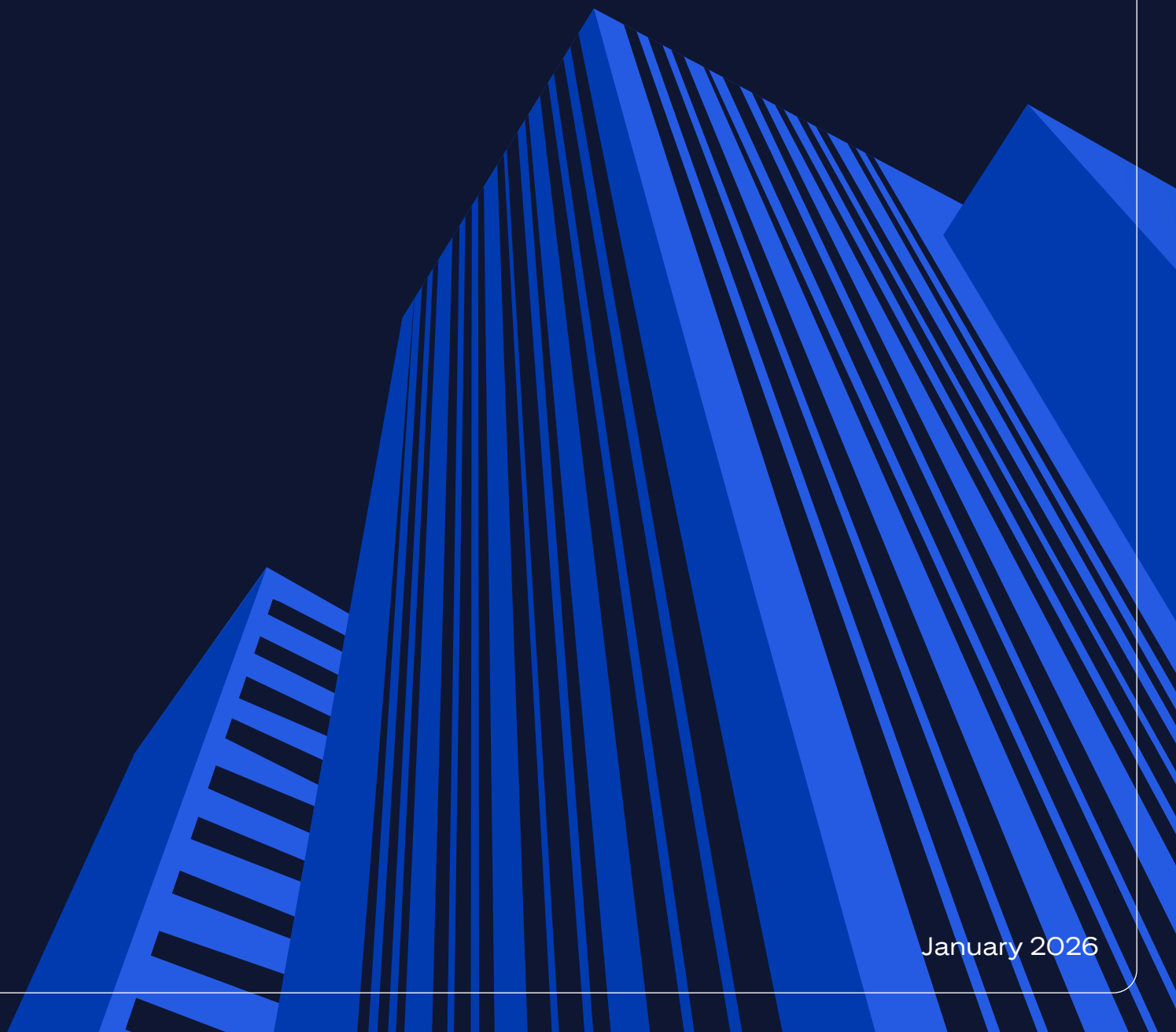
Citi Institute

Quantum Threat

The Trillion-Dollar Security Race Is On



January 2026

Key Takeaways

Post-quantum cryptography is key to combatting quantum threats

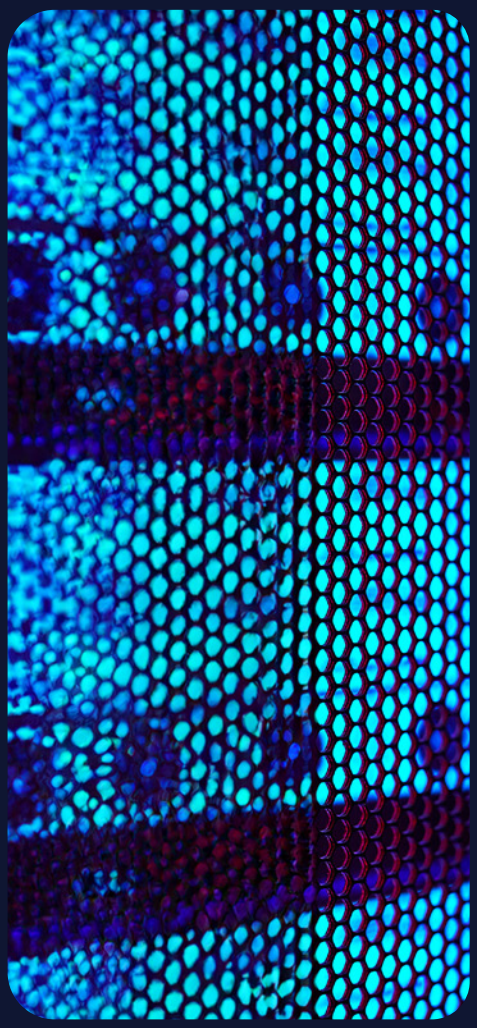
The challenge is not the lack of a solution, but the difficulty of implementing the right solution at scale. For data that requires long-term confidentiality, retroactive cracking of encryption makes action now urgent.

Vulnerable systems must move to quantum-safe alternatives

Quantum readiness starts with a clear sequence of actions that identify exposure, prioritize critical systems, enable agility, guide migration and sustain long-term resilience.

Crypto's quantum risks need addressing

For Bitcoin, public key exposure applies to only about 25% of coins. For other blockchains, the majority of coins are vulnerable. But these newer blockchains can move faster.



19-34%

Probability of widespread breaking of quantum computer-led public-key encryption by 2034, increasing to 60-82% by 2044[1]

$2.0-$3.3tn

Estimated indirect impact (GDP-at-risk) from a single-day quantum attack on one top-five U.S. bank's access to Fedwire, i.e. 10-17% of GDP[2]

25%

The percentage of bitcoins (about 4.5-6.7 million coins worth $500-600 billion today) that are potentially "quantum-exposed"[3]

Quantum Threat

How Far Are We from Q-Day?

The quantum threat stems from a revolutionary shift in computing power. Unlike classical computers that process information sequentially using bits (0 or 1), quantum computers employ "qubits" that can represent 0, 1, or both simultaneously (Citi GPS: Quantum Computing – Moving Quickly from Theory to Reality).

This allows quantum computers to perform certain calculations, particularly those required to break today's complex encryption standards, at speeds that are orders of magnitude faster than any supercomputer imaginable.

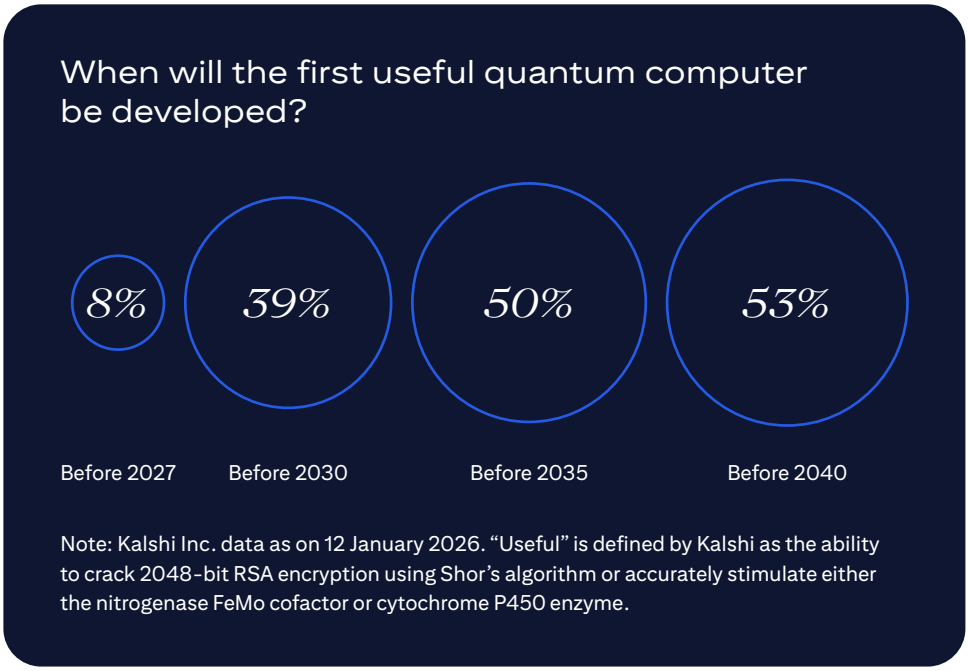
This isn't an evolutionary improvement; it's a fundamentally different computational paradigm that redefines what is possible, making the need to prepare for "Q-day" both urgent and unprecedented.

Q-day refers to the future date when quantum computers become powerful enough to break widely used public-key encryption. The economic and geopolitical consequences of not preparing for Q-day could be severe as it would result in the disruption of current digital security.

Estimates, quoted by U.S. regulators and the Global Risk Institute, place the probability of a Q-day by 2034 at 19-34%, increasing to 60-82% by 2044.[4] Timeline estimates for Q-day vary significantly.

The Kalshi prediction markets, based on aggregated trades, imply a roughly 40% probability of a useful quantum computer by 2030. Many experts believe a cryptographically relevant quantum computer (CRQC) in the 2020s is highly unlikely.[5,6]

However, Q-day is not a sudden on/off event. The threat is already active through harvest-now, decrypt-later attacks, where adversaries store encrypted data today for future quantum decryption.



In our view, organizations that rely on digital encryption and require long timelines for information privacy, should focus now on implementing established post-quantum cryptography (PQC) standards.

And for organizations interacting with governments or in highly regulated industries, such as financial services, PQC compliance will not be an option. There are no hard regulatory requirements to guard against the quantum threat as yet, but regulators are strongly pushing planning and risk management.

For instance, defense agencies and contractors in the U.S. are expected to adopt PQC for anything newly purchased, developed or contracted after 2027; the target for full migration across defense and national security systems is 2035.[7]

With rapid technological improvements and heightened national security, regulatory and policy maker vigilance, we believe quantum computing is rapidly moving from being a science research topic to becoming a boardroom issue.

Even a low probability of Q-day occurring in the next 10 years could result in a serious outcome in the public sector or in financial transactions. Q-day is a classic low-probability but high-severity event.

The good news? Post quantum cryptography standards are available, meaning the antidote to quantum risk is available today. The challenge is not the lack of a solution, but the difficulty of implementing it at scale.

The real Q-day may occur before the world becomes aware of it, as states or bad actors potentially seek to use this knowledge to their strategic advantage.

Quantum computing is part of the mix of emerging technologies, including artificial intelligence, that will have significant geopolitical implications in the years ahead.[8]

Why Now?

Quantum computers have been researched for decades, but the practical security implications have shifted materially in recent years, driven by a combination of factors:

1. Hardware advances
Quantum hardware is improving, with gains in qubit stability, longer coherence times and more effective error suppression driving steady increases in practical performance.

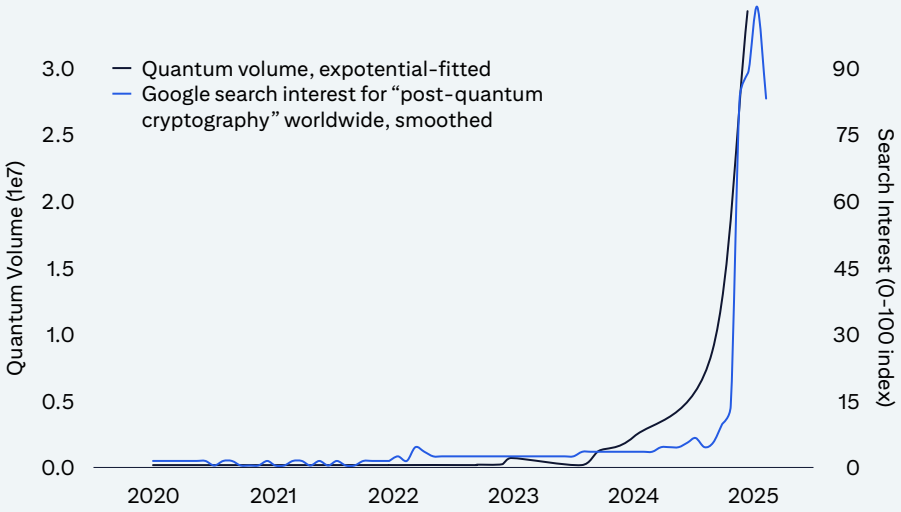
Progress in processor architectures signals movement beyond purely experimental machines toward platforms increasingly relevant for cryptography.

Figure 1 shows acceleration in a quantum computer's overall power (measured by quantum volume), alongside a marked rise in online interest in post-quantum cryptography over the past year.

2. Standards and regulatory momentum
Regulations are a strong accelerant for PQC adoption and regulators are shifting focus from awareness to implementation (see box).

> Quantum computing will reshape our economy and security in the decades ahead... History will not forgive us if we fall behind in the quantum race.
>
> *Rt Hon. William Hague, Chancellor, University of Oxford*

Figure 1. Increase in quantum power and post-quantum cryptography search interest



Note: [1] Quantum volume is a single benchmark metric for assessing the practical performance of a quantum computer by combining qubit count, quality, and error rates. [2] Google search interest sourced from Google Trends using worldwide data.

Source: Google Trends, QuSecure, Citi Institute

Current regulatory initiatives

NIST standards: The U.S. National Institute of Standards and Technology (NIST) has emerged as the de facto global standard-setter for post-quantum cryptography (PQC). In 2024-2025, NIST published three standards: FIPS 203 (ML-KEM); FIPS 204 (ML-DSA); FIPS 205 (SLH-DSA).[9]

NIST is also evaluating additional algorithms, including FIPS 206 (FN-DSA/FALCON) and FIPS 207 (HQC-KEM).[10]

While there is no single mandated date for PQC adoption across institutions, U.S. federal agencies must begin migration of high-risk systems to PQC by 2030 and achieve full quantum-resistant security by 2035.[11]

U.S. executive orders: The January 2025 executive order sets out timelines for PQC adoption across federal agencies.[12] This includes preparing for transition to PQC and requiring the Cybersecurity and Infrastructure Security Agency (CISA) to publish a list of product categories where PQC capabilities are available within 180 days. Post publication, federal agencies must ensure PQC support in new procurements for those categories in 90 days. The order also sets 2030 as a milestone for federal systems to support Transport Layer Security (TLS) 1.3 or later, which is considered the foundation for PQC integration.

European Union (EU) guidance: In June 2025, EU member states, supported by the European Commission, issued coordinated roadmaps and minimum requirements for the PQC transition. Member states must start national PQC transition strategy by end of 2026 and high-risk systems transitioned by end of 2030.[13]

The EU Quantum Act, expected to be adopted in 2026, is anticipated to formalize Europe's policy, funding and governance framework for quantum technologies.[14]

Israel directive: In January 2025, the Bank of Israel issued a letter, under the Proper Conduct of Banking Business Directive 364, mandating banking corporations and licensed payment service providers to assess and manage cyber risks arising from quantum computing capabilities. Institutions must map encrypted information assets and develop an initial preparedness plan within one year of the letter's issuance – the deadline is looming.[15]

Other jurisdictions: The UK, Canada, Australia, France, Germany, the Netherlands, Norway, Japan, South Korea, China and Russia are actively developing or recommending PQC standards, policies and transition timelines. Many are aligning with NIST, while others are pursuing parallel national frameworks.

3. Rising security concerns

The most acute quantum risk does not lie in future attacks, but in the current "harvesting" (i.e., archiving) of encrypted data that can be stored now and decrypted by bad actors in the future when a cryptographically relevant quantum computer (CRQC) arrives. Harvest now, decrypt later (HNDL) is an immediate and systemic threat of the quantum era.

This threat is particularly severe for data with a long shelf live, such as social security numbers, biometric authentication data, medical records, intellectual property and long-term confidential government or defense information.

Recent assessments by the U.S. Federal Reserve[16] have highlighted that while organizations must transition to quantum-safe protections, doing so only protects future data flows. Historical privacy loss cannot be reversed. The only inherent safeguard against this historical privacy loss is that the need for data secrecy must expire before powerful quantum computers arrive.

How Quantum Threatens Today's Cryptography

The core concern is that powerful quantum computers could break today's widely used cryptographic standards. This could compromise sensitive data across sectors such as defense, energy, finance, healthcare and critical infrastructure. Some key risks posed by quantum computers include:

Breaking public-key encryption: The immediate risk is to asymmetric encryption. A sufficiently advanced quantum computer using Shor's algorithm could compromise commonly used encryption algorithms like Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC).

Symmetric encryption such as AES is considered less vulnerable, as quantum computers cannot solve its underlying mathematical problems as efficiently. To strengthen security, companies can adopt AES-256, instead of AES-128, although the shift can be arduous due to system and compatibility updates.

Compromising digital signatures and identity: Digital signatures confirm integrity and authenticity. If quantum computers can obtain private keys, they can forge signatures convincingly. Attackers could impersonate trusted software vendors, push malicious updates or access systems unnoticed.

Compromising encryption and digital signatures will lead to significant collateral damage. We list some examples:

> Q-Day is often treated as a future event. From a risk perspective, it is already here. Data stolen today can be decrypted later. Organizations don't need quantum systems to respond; PQC is deployable today.
>
> *Rebecca Krauthamer, Co-Founder and CEO, QuSecure*

Exposing IoT ecosystems: Most Internet of Things (IoT) devices often use lightweight encryption designed for efficiency, not quantum resistance. With over 20 billion globally active IoT devices estimated in 2025,[17] the quantum threat is real. Many IoTs are also difficult to update once deployed. The long replacement cycle makes large, distributed IoT networks vulnerable to quantum attacks.

Weakening secure communications: Technologies like TLS, HTTPS, VPNs and email encryption rely on public-key exchange (also knowns as asymmetric cryptography). Quantum-enabled adversaries could decrypt traffic, impersonate users or intercept credentials in transit. This could result in loss of confidentiality and authenticity across global communication systems.

Endangering critical infrastructure: Operational technology and industrial control systems often use long-lived hardware and cryptographic keys. Quantum attacks could jeopardize essential sectors like energy, finance, telecom and healthcare if migration lags.

Creating geopolitical imbalance: Nations or organizations that achieve cryptographically relevant quantum capability first will gain disproportionate intelligence and defense advantages. Encrypted diplomatic, military and economic data from other nations could be exposed.

Threatening blockchains: Quantum computers do not undermine the blockchain ledger but could undermine cryptography securing transaction validation.

Most public blockchains depend on elliptic curve cryptography (ECC) for digital signatures. A sufficiently powerful quantum computer could recreate

private keys and falsify transactions, undermining immutability and trust across the blockchain.

Economy-wide Exposure

The economic and operational implications of quantum attacks are broad, as today's digital world relies extensively on public-key cryptography. If bad actors gain the ability to break it, the exposure extends across every layer of modern infrastructure.

A successful quantum attack would not be limited to one institution or sector but rather have a contagion effect across sectors. Systems that protect digital signatures, authentication tools and high-value data would be more vulnerable.

Government and defense: Government agencies and defense systems are prime targets for espionage, disruption, and strategic information collection. Quantum enabled attacks could decrypt diplomatic communication, military strategies, or classified archives, undermining national security.

Finance and banking: Financial institutions hold vast amounts of transaction data, authentication credentials and sensitive personal information that relies on cryptographic security. A quantum attack could compromise payment systems, digital identities, interbank messaging and more. Beyond direct theft, the broader economic impact could echo through the wider economy.

Healthcare: Electronic health records contain sensitive patient records, identity information and long-term medical histories. These assets remain valuable for decades, making them prime targets for harvest-now, decrypt-later attacks.

Telecommunications: Telecom providers operate critical communication infrastructure that enables the functioning of other sectors. A quantum breach could disrupt core routing of communication channels across the economy.

Impact Could Be in the Trillions

Data breaches are already a significant cyber challenge, with global average cost per data breach estimated at $4.4 million in 2025.[18]

Quantifying the dollar value of a quantum attack can be challenging with some estimates suggesting multi-trillion dollars in digital value being exposed in a post Q-day scenario.

A 2023 study demonstrates a single-day quantum attack on one of the five largest U.S. financial institutions, aimed at their access to the Fedwire Funds Service payment system, could trigger a cascading financial failure costing the U.S. economy between $2.0-3.3 trillion in indirect impacts alone, as measured by GDP-at-risk. This translates to a decline in annual real GDP in the range of 10% to 17%, beginning with the initial attack scenario and lasting through the resulting six-month recession.[19]

However, the true economic cost could ultimately reflect the value of every digital interaction or asset that relies on classical cryptography, making the potential impact far larger than any previous cybersecurity risk.

Cost of upgrades? The cost of transitioning to quantum-safe cryptography varies widely depending on the size and complexity of the system. Software followed by hardware upgrades form a large part of the spend, but the real cost extends beyond technology. Companies need to invest in re-engineering interfaces and authentication layers, retrain staff and fund large-scale migration programs. For global institutions, these efforts could stretch across thousands of applications and multi-year change cycles.

> Quantum computing will trigger the largest upgrade of cryptography in human history, far bigger than the Y2K transition.
>
> *Steve Suarez, CEO of HorizonX and Senior Advisor, McKinsey & Company*

Looking back, the Y2K remediation effort in the late 1990s was the last comparable global software overhaul. Estimates suggest global spend at $300-600 billion then,[20] which in today's money is closer to $600 billion-1.1 trillion.

Yet Y2K was a relatively contained problem with a clear deadline and finite scope. The quantum shift is far broader, requiring a complete overhaul of digital infrastructure to replace every piece of classical encryption. This could make the eventual upgrade bill potentially much larger and more unevenly distributed across sectors.

> Quantum risk does not merely threaten crypto primitives. It challenges the ideological foundations of crypto itself. As the assumptions behind immutability and decentralized trust weaken, quantum computing accelerates the unravelling of a story that was always more vulnerable than its proponents admitted. Perhaps a warning for all our human systems.
>
> *Daniel Doll-Steinberg, Co-founder and Head of Strategy, Edenbase*

What Should Institutions Do?

Quantum computing is no longer just a topic reserved for scientists. It is now an operational and strategic risk for institutions, especially those that rely on public-key cryptography to secure communications, data and authentication. Emerging regulations require institutions to ensure their systems are quantum resistant.

Institutions must move from curiosity to structured quantum-readiness programs, setting short and long-term goals to manage risk. Key measures for institutions to implement:

Strengthen cryptographic foundations: New applications must be developed in line with modern encryption standards. Institutions must design systems natively around PQC algorithms laid out by bodies such as the NIST, Internet Engineering Task Force (IETF) and Accredited Standards Committee X9 (ANSI X9). These are now becoming the default baseline for new application development.

Build crypto-agile systems: Crypto-agility refers to the ability of systems to switch cryptographic mechanisms and algorithms quickly in response to changing threats, vulnerabilities or technological advances. For large institutions with complex systems, this capability is essential, as it reduces future migration costs and makes it easier to incorporate post-quantum algorithms once the standards mature.

Deploy quantum-safe shields for immediate protection: Replacing cryptographic components across a large organization is a multi-year effort. In the meantime, institutions can deploy a quantum-safe shield or network overlays that offer immediate protection against harvest-now, decrypt-later risks. These overlays place a quantum-resistant encryption layer around all inbound and outbound data flow without requiring changes to underlying applications. These measures can act as a rapid defence measure while longer-term cryptographic updates proceed internally.

Five-Point Execution Plan for Quantum-Safe Migration

To manage the shift to quantum-resistant systems, institutions need a structured approach built around five key steps. These steps are not a linear or sequential critical path. In practice, identification, prioritization and migration should progress in parallel. Organizations should begin piloting post-quantum migration early, rather than wait for inventories and strategies to be fully completed.

1. **Identify** where public-key cryptography is used across the organization
2. **Prioritize** critical systems and long-lived data that requires immediate migration (e.g., identity systems, payment infrastructure, digital signatures)
3. **Enable** crypto-agility and hybrid approaches that allow classical and post-quantum algorithms to operate side-by-side
4. **Migrate** by executing a phased transition plan spread over several years, aligned with vendors' readiness and regulatory guidance
5. **Sustain** continuous key management and rotation to respond quickly to new PQC standards and replace vulnerable algorithms as quantum capabilities evolve

> A quantum readiness program must prioritize protecting clients/assets through a holistic uplift of internal systems and data protection to counter the harvest-now, decrypt-later threats, along with proactive engagement with vendors and partners on migration roadmap alignment.
>
> *Sebastian Ganson, Chair–Cryptographic Security Center of Excellence, Citi*

Adopt quantum-ready cloud computing: Cloud platforms could provide a fast route for institutions to test and adopt quantum technologies. Accessing quantum capabilities through the cloud reduces the need for specialized hardware and facilitates early pilots. Major cloud providers are integrating quantum-safe cryptography into their infrastructure, which could help institutions make PQC migration quicker and less costly than upgrading on-premises systems.

Collaborate across the ecosystem: No institution can become quantum secure in isolation. Security depends on multiple participants including cloud providers, hardware vendors, software partners, telecom networks and global supply chains. This can be a complex problem especially for large institutions with multiple vendors and suppliers. Vendors must strengthen their cryptographic foundations in line with their client's timelines and priorities, ensuring that no gaps in strategically implementing PQC solutions exist for any of their end-users.

Address key challenges: Quantum preparedness can be complicated by the presence of large, ageing technology with decades of custom integrations. Institutions with significant on-premises hardware could find it harder to implement PQC internally, whereas cloud providers may adopt quantum-safe methods sooner.

There is also a widening skills gap. Institutions need to hire or retrain teams in quantum-safe architecture and risk modelling.

Quantum Risk for Blockchains

Quantum computers threaten blockchains by undermining the public-key cryptography used to validate transactions. If attackers can derive private keys from exposed public keys using Shor's algorithm, they can sign transactions, move funds, or impersonate legitimate owners.

The quantum computing risk for blockchains (excluding so-called privacy coins) is based on the breaking of digital signatures, and not encryption. The limited exposure to HNDL risk for blockchains, compared to governments or banks, gives them a longer timeline to manage the transition to PQC.

The quantum risk to digital signatures is not necessarily imminent, as many experts expect cryptographically relevant quantum computers to be at least a decade away, with large uncertainty. However, once such machines exist, any funds controlled by a key whose public key is already exposed on-chain would be vulnerable.

In blockchains such as Bitcoin, public key exposure only applies to a subset of coins, about 25%. For other blockchains, the majority of the coins are vulnerable. For ETH, over 65% of current supply is vulnerable.[21] For SOL, it is effectively all the supply at risk. Not surprisingly, public-key exposed chains are planning migration paths already.

While the Bitcoin blockchain is less vulnerable to public key exposure, it faces a special headache around governance and abandoned coins as noted by Justin Thaler of a16z crypto.[22] Governance speed is slow and Bitcoin changes slowly. And migration to post-quantum signatures can't be passive. Which means abandoned coins are quantum vulnerable.

Taking Bitcoin as an illustration, the system relies on two core primitives: SHA-256 for hashing and the ECDSA signature scheme based on elliptic-curve cryptography (ECC) for digital signatures. While SHA-256 is considered relatively resilient, ECDSA would be vulnerable.

The ECDSA security model assumes that although the public key is visible, the private key cannot be derived from it. A sufficiently powerful quantum computer running Shor's algorithm could invalidate this assumption.

Two points of vulnerability emerge:

1. When bitcoin is spent, the public key appears in the mempool,[23] before the transaction is confirmed on-chain. In this window, a quantum computer could derive the private key and redirect the funds.
2. Early bitcoin transactions used Pay-to-Public-Key (P2PK) outputs, which store the public key directly on-chain. Along with Taproot outputs and reused addresses whose public keys have been revealed, these so-called 'quantum-exposed' outputs hold an estimated 4.5–6.7 million BTC (on the order of $500–600 billion today). This includes a large fraction of early coins, likely including Satoshi's.

CRQCs are not generally expected to be fast enough to derive private keys during the window in which public keys are exposed in the mempool. Hence, the more immediate concern, once CRQCs exist, is the large pool of coins whose public keys are already on-chain today. Those can be attacked offline over long periods.

Newer address formats like Pay-to-Public-Key-Hash (P2PKH) reduce exposure by hashing the public key. However, once funds are spent, the underlying public key is revealed again revealed and becomes vulnerable. Avoiding address reuse can reduce exposure by limiting how often public keys are revealed.

These vulnerabilities are not limited to Bitcoin. Many blockchains rely on similar elliptic curve cryptography, meaning the underlying quantum risk extends across the ecosystem.

What can be done? Chains must upgrade their cryptography to PQC standards. Leading blockchains are already researching/prototyping post-quantum signature schemes including lattice-based algorithms such as Crystals-Dilithium and Falcon, and hash-based schemes like SPHINCS+.

A key step is to map existing addresses, particularly those where public keys have already been revealed on-chain, to prepare for large-scale migration once quantum-safe standards are implemented. Address format or transaction flow that expose public keys before or during spending increase the attack surface and require redesign as part of the transition.

Approaches vary by network design and governance. For example, Bitcoin's upgrade path is incremental and consensus -driven, with post-quantum discussions focusing on introducing new address or script types via soft forks, alongside extended transition periods for existing outputs.

Ethereum's governance and hard-fork mechanism allow protocol-level cryptographic changes, while ongoing work on account abstraction and signature flexibility could support the coexistence of multiple signature schemes over time.

Solana has explored post-quantum signature verification and migration concepts through research and testnet experimentation, assessing how quantum-resistant schemes might operate within a high-throughput execution environment.

Custody platforms and wallet providers also need robust key rotation infrastructure to support seamless migration as post-quantum standards are adopted. And even if underlying blockchains, platforms and wallets upgrade to PQC over time, we ultimately need a social consensus around technology upgrades, implementation and adoption.

> Blockchain systems today operate reliably under current cryptographic assumptions. However, quantum computing introduces a deferred risk comparable to a vehicle that continues to run despite compromised tires – functionally adequate for now, yet vulnerable to abrupt failure once stress thresholds are exceeded.
>
> *Christian Papathanasiou, Chief Architect, Quantum Bitcoin*

Glossary

We list and explain some key terms and concepts associated with Quantum Technology that appear in this paper. Where applicable, we also provide relevant examples.

Q-day: A future date when quantum computers become powerful enough to break widely used public-key encryption. Estimated times vary.

Qubit (Quantum bit): Basic unit of quantum information (quantum counterpart to a classical computer's bit). Qubits are physical systems such as single atoms, photons, trapped ions, etc. Due to quantum properties such as superposition, Qubits can hold more complex information enabling powerful parallel computations for certain problems.

Physical/Logical Qubit: Physical qubits are the actual, noisy quantum bits (like photons, trapped ions, etc.) in hardware, while a logical qubit is an error-corrected, robust, virtual qubit created by encoding one logical bit's information across many entangled physical qubits, forming the foundation for fault-tolerant quantum computing.

Digital Signatures: A cryptographic method for verifying the authenticity and integrity of a digital message or document. Progress in quantum computing threaten today's signature schemes (Rivest-Shamir-Adleman (RSA), Elliptic Curve Digital Signature Algorithm (ECDSA)), making PQC signatures a key requirement.

Hashing/Hash Value: A one-way mathematical process that transforms any input data into a fixed-length string of characters called a hash value or message digest. Current robust hashing algorithms like SHA-256 are expected to remain relatively resistant to current and near-future quantum attacks. Researchers are also developing specific quantum-resistant hashing schemes and hash-based signatures to prepare for a post-quantum world.

Cryptographically Relevant Quantum Computer (CRQC): A future quantum computer powerful enough to run algorithms like Shor's algorithm, breaking most current public-key encryption (like RSA, Elliptic Curve Cryptography (ECC)) that secures online banking, communications, and digital signatures.

Public-Key Infrastructure (PKI): System of technologies, supporting processes and underlying governance used to manage (create, distribute, revoke) digital certificates and Public-key Encryption (PKE). PKI underpins identity/ authentication systems (e.g. secure email) and is the main infrastructure that must be upgraded to PQC.

Post-Quantum Cryptography (PQC): Cryptographic algorithms that are designed to resist attacks from quantum computers. Organizations like the National Institute of Standards and Technology (NIST) are standardizing these algorithms to prepare for the quantum era. PQC is the primary defence against Q-Day.

NIST PQC Standards: The National Institute of Standards and Technology (NIST) are standardizing cryptographic algorithms to prepare for the quantum era. Organizations are expected to migrate to these standards before Q-Day. Examples include FIPS 203 (ML-KEM); FIPS 204 (ML-DSA); FIPS 205 (SLH-DSA).[24] NIST is also evaluating additional algorithms, including FIPS 206 (FN-DSA/FALCON) and FIPS 207 (HQC-KEM).[25]

Harvest Now, Decrypt Later (HNDL): Attackers intercept encrypted traffic today and store it with the explicit aim of decrypting it for malicious use once sufficiently powerful quantum computers become available. Evergreen, highly sensitive information with long-term value are potential targets. Examples include Personal Identifiers such as Social Security numbers, medical records (PHI), and other data useful for long-term identity theft.

Authors

Ronit Ghose
Global Head, Future of Finance, Citi Institute
ronit.ghose@citi.com

Sophia Bantanidis
Future of Finance, Citi Institute
sophia.bantanidis@citi.com

Prag Sharma
Future of Finance, Citi Institute
prag.sharma@citi.com

Ronak Shah
Future of Finance, Citi Institute
ronak.sharad.shah@citi.com

Kaiwan Master
Future of Finance, Citi Institute
kaiwan.hoshang.master@citi.com

Contributors

Alex McMahon
Citi Innovation Labs

Christian Papathanasiou
Quantum Bitcoin

Ciaran Fennessy
Citi Services Technology

Daniel Doll-Steinberg
Edenbase

Garrison Buss
QuSecure

Justin Thaler
a16z crypto

Loreal Andrews
Citi CISO – Client Cybersecurity

Rebecca Krauthamer
QuSecure

Robert Rowe
Citi Research

Rt Hon. William Hague
University of Oxford

Sarah McCarthy
Citi Cryptographic Security Center of Excellence

Sebastian Ganson
Citi Cryptographic Security Center of Excellence

Steve Suarez
HorizonX

Sudha E Iyer
Citi Enterprise PKI & Cryptography Engineering

Tahmid Quddus Islam
Citi Innovation & Technology

Thank you to all contributors. The conclusions and views are those of the Citi Institute and the named authors.

Endnotes

[1] Global Risk Institute (GRI), Quantum Threat Timeline Report 2024, 06 December 2024.

[2] Hudson Institute, Prosperity at Risk: The Quantum Computer Threat to the US Financial System, 03 April 2023.

[3] Deloitte, Quantum Risk To The Ethereum Blockchain – A Bump In The Road Or A Brick Wall?, 2022.

[4] Global Risk Institute (GRI), Quantum Threat Timeline Report 2024, 06 December 2024.

[5] A16zcrypto (Justin Thaler), Quantum Computing and Blockchains: Matching Urgency To Actual Threats, 12 December 2025.

[6] Global Risk Institute (GRI), Quantum Threat Timeline Report 2024, 06 December 2024.

[7] US National Security Agency, Announcing the Commercial National Security Algorithm Suite 2.0, May 2025.

[8] Tony Blair Institute for Global Change, A New National Purpose: A UK Quantum Strategy for Sovereignty and Scale, 03 November 2025.

[9] The National Institute of Standards and Technology (NIST) News, Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography, 13 August 2024.

[10] The National Institute of Standards and Technology (NIST) News, NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption, 11 March 2025.

[11] The National Institute of Standards and Technology (NIST) IR 8547, Transition to Post-Quantum Cryptography Standards, 2024.

[12] The White House, Executive Order on Strengthening and Promoting Innovation in the Nation's Cybersecurity, 16 January 2025.

[13] European Commission, A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, 11 June 2025.

[14] European Commission, Commission Invites Contributions to Shape Future EU Quantum Act, 31 October 2025.

[15] The Bank of Israel, Banking System Preparedness for Cyber Risks Arising from Quantum Computing Capabilities, 07 January 2025.

[16] Federal Reserve Board, "Harvest Now Decrypt Later": Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Network, September 2025.

[17] IoT Analytics, State of IoT 2025: Number of Connected IoT Devices Growing 14% to 21.1 Billion Globally, 28 October 2025.

[18] IBM Report, Cost of a Data Breach Report 2025: The AI Oversight Gap, August 2025.

[19] Hudson Institute, Prosperity at Risk: The Quantum Computer Threat to the US Financial System, 03 April 2023.

[20] Smithsonian, The National Museum of American History, Y2K, Last Accessed 11 September 2019.

[21] Deloitte, Quantum Risk To The Ethereum Blockchain – A Bump In The Road Or A Brick Wall?, 2022.

[22] A16zcrypto (Justin Thaler), Quantum Computing and Blockchains: Matching Urgency To Actual Threats, 12 December 2025.

[23] A bitcoin mempool (memory pool) can be thought of as a waiting room for unconfirmed transactions held in the network node's memory, before miners pick them up to include in a new block.

[24] The National Institute of Standards and Technology (NIST) News, Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography, 13 August 2024.

[25] The National Institute of Standards and Technology (NIST) News, NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption, 11 March 2025.

For digital accessibility support, please contact your Citi Team for immediate queries, or email accessibility@citi.com.
You may visit Accessibility at Citi | Citi.com for more information.

IMPORTANT DISCLOSURES

This communication has been prepared by Citigroup Global Markets and is distributed by or through its locally authorised affiliates (collectively, the "Firm"). This communication is not intended to constitute "research" as that term is defined by applicable regulations, though it may contain thematic content that has been or may be contained in research reports. Unless otherwise indicated, any reference to a research report or research recommendation is not intended to represent the whole report and is not in itself considered a recommendation or research report. The views expressed by each author herein are their personal views and do not necessarily reflect the views of their employer or any affiliated entity or the other authors, may differ from the views of other personnel at such entities, and may change without notice. You should assume the following: The Firm may be the issuer of, or may trade as principal in, the financial instruments referred to in this communication or other related financial instruments. The author of this communication may have discussed the information contained herein with others within the Firm and the author and such other Firm personnel may have already acted on the basis of this information (including by trading for the Firm's proprietary accounts or communicating the information contained herein to other customers of the Firm). The Firm performs or seeks to perform investment banking and other services for the issuer of any such financial instruments. The Firm, the Firm's personnel (including those with whom the author may have consulted in the preparation of this communication), and other customers of the Firm may be long or short the financial instruments referred to herein, may have acquired such positions at prices and market conditions that are no longer available, and may have interests different or adverse to your interests. This communication is provided for information and discussion purposes only. It does not constitute an offer or solicitation to purchase or sell any financial instruments. The information contained in this communication is based on generally available information and, although obtained from sources believed by the Firm to be reliable, its accuracy and completeness is not guaranteed. Certain personnel or business areas of the Firm may have access to or have acquired material non-public information that may have an impact (positive or negative) on the information contained herein, but that is not available to or known by the author of this communication. The Firm shall have no liability to the user or to third parties, for the quality, accuracy, timeliness, continued availability or completeness of the data nor for any special, direct, indirect, incidental or consequential loss or damage which may be sustained because of the use of the information in this communication or otherwise arising in connection with this communication, provided that this exclusion of liability shall not exclude or limit any liability under any law or regulation applicable to the Firm that may not be excluded or restricted. The provision of information is not based on your individual circumstances and should not be relied upon as an assessment of suitability for you of a particular product or transaction. Even if we possess information as to your objectives in relation to any transaction, series of transactions or trading strategy, this will not be deemed sufficient for any assessment of suitability for you of any transaction, series of transactions or trading strategy. The Firm is not acting as your advisor, fiduciary or agent and is not managing your account. The information herein does not constitute investment advice and the Firm makes no recommendation as to the suitability of any of the products or transactions mentioned. Any trading or investment decisions you take are in reliance on your own analysis and judgment and/or that of your advisors and not in reliance on us. Therefore, prior to entering into any transaction, you should determine, without reliance on the Firm, the economic risks or merits, as well as the legal, tax and accounting characteristics and consequences of the transaction and that you are able to assume these risks. Financial instruments denominated in a foreign currency are subject to exchange rate fluctuations, which may have an adverse effect on the price or value of an investment in such products. Investments in financial instruments carry significant risk, including the possible loss of the principal amount invested. Investors should obtain advice from their own tax, financial, legal and other advisors, and only make investment decisions on the basis of the investor's own objectives, experience and resources. This communication is not intended to forecast or predict future events. Past performance is not a guarantee or indication of future results. Any prices provided herein (other than those that are identified as being historical) are indicative only and do not represent firm quotes as to either price or size. You should contact your local representative directly if you are interested in buying or selling any financial instrument, or pursuing any trading strategy, mentioned herein. No liability is accepted by the Firm for any loss (whether direct, indirect or consequential) that may arise from any use of the information contained herein or derived herefrom. Although the Firm is affiliated with Citibank, N.A. (together with its subsidiaries and branches worldwide, "Citibank"), you should be aware that none of the other financial instruments mentioned in this communication (unless expressly stated otherwise) are (i) insured by the Federal Deposit Insurance Corporation or any other governmental authority, or (ii) deposits or other obligations of, or guaranteed by, Citibank or any other insured depository institution. This communication contains data compilations, writings and information that are proprietary to the Firm and protected under copyright and other intellectual property laws, and may not be redistributed or otherwise transmitted by you to any other person for any purpose.

26-9D21C18F 01/26