Preparing for the Quantum Era: Assessing Quantum Computing Risks to Blockchain Security

Duc V. Le, Panos Chatzigiannis, Navid Alamati, Sunpreet Singh Arora, Anderson Nascimento, Timothy Conard, Noah Levine, Adam Clark, Cuy Sheffield

Visa Research and Visa Crypto

January 2026

Executive Summary

Quantum computers pose a direct threat to the cryptographic foundations securing all major blockchains, including Bitcoin, Ethereum, and Solana, as well as systems underpinning over $272 billion in stablecoins as of January 2026 [5]. While this threat is not imminent, the timeline is uncertain, and the window for preparation may narrow over time. The good news: quantum-resistant cryptographic solutions exist and have been standardized. The challenge lies in migrating complex, decentralized blockchain systems before quantum computers become powerful enough to exploit current vulnerabilities. This migration will require years of coordinated effort across the global digital asset ecosystem, which suggests that early preparation is worth consideration.

Key Takeaways

1. **The quantum threat timeline remains uncertain.** Estimates range widely, but preparation may need to begin well in advance, as migration can take years.
2. **Stablecoins face concentrated risk.** Unlike individual users who can distribute funds across many wallets, stablecoin issuers operate through a small number of highly visible addresses, creating an unusually concentrated attack surface.
3. **Migration requires multi-year coordination.** Blockchain protocol upgrades require extensive design, testing, and coordination across thousands of independent node operators, wallet providers, and institutions, as demonstrated by Ethereum's transition to proof-of-stake.
4. **NIST standards provide partial coverage.** Standards cover basic signatures and key exchange, but blockchain-specific primitives (ZK proofs, VRFs, threshold signatures) require dedicated research, and the blockchain community has historically chosen algorithms outside NIST selections.

5. **Migration is costly.** Quantum-safe cryptography adds overhead, and modular migration strategies are being explored as a way to manage transition costs across heterogeneous ecosystems.
6. **Privacy loss is retroactive.** Historical transaction data cannot be re-protected once revealed.
7. **Proof-of-stake chains face additional risks.** The ability to forge historical validator signatures enables history-rewriting attacks.
8. **Early preparation is an active area of discussion.** Researchers and industry participants are examining activities such as cryptographic dependency mapping, key management hardening, edge-level experimentation, and protocol upgrade planning.

This report provides a comprehensive assessment of quantum threats to blockchain security, explains why stablecoins deserve special attention, and outlines practical steps the ecosystem can take to prepare for the quantum era.

Understanding the Quantum Threat to Blockchain Security

The security foundations of blockchains have held up under classical threat models, but quantum computing introduces a fundamentally different kind of threat.

How Quantum Computers Break Blockchain Security

The core vulnerability lies in widely used asymmetric-key cryptography, particularly digital signature and public-key encryption schemes whose security relies on the hardness assumption of specific mathematical problems. For example, RSA relies on the infeasibility of integer factorization, while DSA, ECDSA, and EdDSA are based on the difficulty of the discrete logarithm problem, including its elliptic-curve variant.

For cryptographically sized keys, these problems are believed to require computational effort far beyond practical limits on classical computers, often estimated as exceeding billions of years. However, this assumption was fundamentally challenged in 1994, when Peter Shor introduced a quantum algorithm capable of solving both integer factorization and discrete logarithms in polynomial time on a sufficiently large, fault-tolerant quantum computer. As a result, the security foundations of these asymmetric cryptosystems would be effectively eliminated in such a quantum setting.

Not all quantum algorithms pose the same level of threat. While Shor's algorithm would compromise public-key cryptography, Grover's algorithm has a more limited impact. Grover's algorithm provides only a quadratic speedup against brute-force search, reducing the effective security of a hash function like SHA-256 from 2^{256} to 2^{128} operations. This reduction does not break hash-based security in practice, as the remaining security margin remains large. In the context of proof-of-work consensus mechanisms, Grover's algorithm would at most provide a modest advantage in mining efficiency, which can be offset through standard parameter adjustments such as increased difficulty or longer hash outputs. As a result, proof-of-work systems are not fundamentally threatened by quantum search algorithms.

Multi-Layer Impact Across the Blockchain Stack

Blockchains are constructed as a three-layer stack, with each layer depending on those below:

- **Application Layer**: Transaction signatures become forgeable, enabling theft from any wallet with an exposed public key. For stablecoins, this means concentrated treasuries and minting keys become vulnerable targets.
- **Consensus Layer**: Validator keys can be derived, allowing attackers to impersonate validators and manipulate block production. On proof-of-stake chains, adversaries could potentially rewrite blockchain histories using forged signatures.
- **Network Layer**: Encrypted node communications can be decrypted and node identities spoofed, enabling traffic analysis and eclipse attacks that isolate portions of the network.

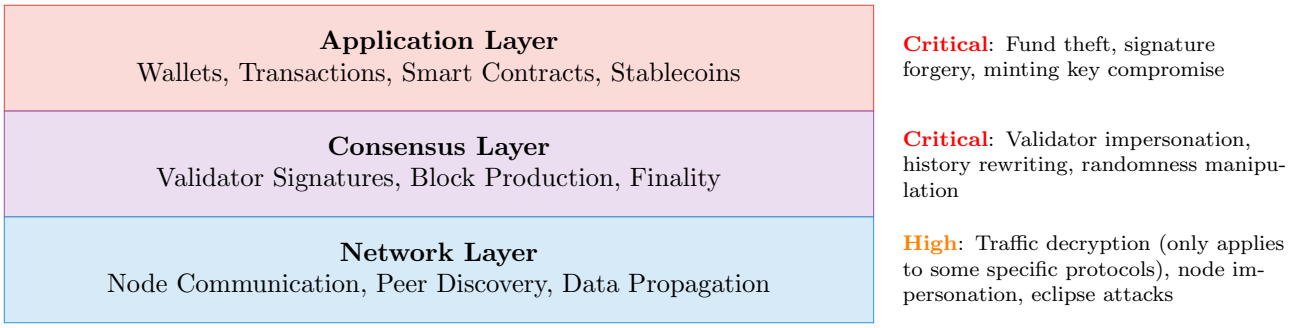

Figure 1: Three-layer blockchain architecture with quantum threat severity by layer.

What Would a Quantum Attack Look Like?

A quantum attack would not appear as a supercomputer suddenly "hacking everything". It would be quieter and more surgical. By breaking the digital signatures that protect accounts, an attacker could authentically impersonate legitimate users and systems.

For everyday users, this means a thief could drain any wallet whose public key is visible on-chain—a category that includes many reused Bitcoin addresses and Ethereum addresses. For stablecoins, the consequences are more severe: if an attacker obtained a stablecoin issuer's minting key, they could create unlimited new tokens and collapse the peg within minutes, potentially destabilizing broader crypto markets.

On proof-of-stake blockchains, the stakes are higher still. A quantum attacker could produce an alternative version of blockchain history that appears completely valid, rewriting past transactions or redirecting funds. Even the underlying network could be targeted: by forging node identities, an attacker could isolate or censor portions of the network. While these scenarios differ in execution, they all stem from the same core vulnerability: if digital signatures break, the entire trust model breaks with them.

Why Stablecoins Deserve Special Attention

Stablecoins occupy a unique position in the digital asset ecosystem that makes them both systemically important and structurally vulnerable to quantum attacks.

Concentrated Value and Attack Surface Unlike individual users who can distribute funds across many wallets, stablecoin issuers often operate through a small number of highly visible on-chain addresses. This creates an unusually concentrated target: if a quantum attacker could forge the signature controlling a stablecoin's minting key, they could create unlimited new tokens, break the peg, and potentially destabilize crypto markets almost instantly.

The scale of exposure is significant. As of January 2026, stablecoins represent over $272 billion in value, much of it concentrated in smart contract addresses with known cryptographic parameters. This concentration creates both a high-value target and a clear attack vector for sophisticated adversaries.

Cross-Chain Exposure and Systemic Risk Stablecoins operate across multiple blockchain networks, meaning a cryptographic weakness in any single chain can compromise the entire stablecoin system. A successful attack on one blockchain could create cascading effects across the interconnected stablecoin ecosystem.

Moreover, stablecoins have evolved beyond cryptocurrency trading. They are increasingly used for payments, remittances, and institutional settlement—functions that connect directly to traditional financial systems. A successful quantum attack on stablecoins would have consequences that extend well beyond crypto exchanges, potentially affecting mainstream payment flows and financial infrastructure.

Regulatory Environment and Trust The regulatory landscape for stablecoins is advancing rapidly. In the United States, the GENIUS Act has established a federal framework for stablecoin issuers with requirements for full reserve backing and supervisory oversight. Similar frameworks are emerging globally, from the EU's MiCA regulations to Singapore's licensing regime.

This increasing regulatory clarity brings stablecoins closer to mainstream financial infrastructure, raising the stakes for security failures. Quantum preparedness is not just a technical consideration; it's becoming a regulatory and institutional trust issue. Financial institutions and regulators will increasingly expect proactive quantum risk management from stablecoin issuers.

In short, stablecoins are both systemically important and structurally vulnerable to quantum attacks, making them the highest-priority asset class to protect as the ecosystem prepares for the quantum era.

Application Layer: Financial Exposure

The scale of potential exposure is substantial. Stablecoins concentrate over $272 billion in known smart contract addresses [5]. An attacker who can forge signatures could drain treasuries or mint unlimited tokens, collapsing the peg instantly.

On Bitcoin, any address that has previously sent a transaction has its public key exposed on-chain. This includes all legacy Pay-to-Public-Key (P2PK) addresses and any Pay-to-Public-Key-Hash (P2PKH) address that has been reused. These funds become vulnerable once quantum computers can derive private keys from public keys.

Proof-of-stake validators on networks like Ethereum and Solana face similar exposure. Compromised validator keys enable not just theft but direct manipulation of consensus mechanisms, potentially allowing attackers to influence which transactions are included in blocks and how network state evolves.

The table below summarizes the threat landscape.

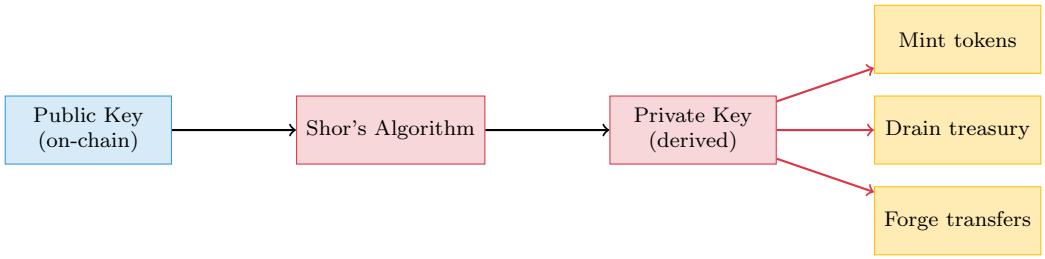

Figure 2: Application-layer attack: deriving a stablecoin minting key via Shor's algorithm enables unlimited token creation and peg collapse.

Asset	Impact	Why It's Vulnerable
Stablecoins (USDT, USDC)	Critical	≈$272 concentrated in known addresses; minting keys are high-value targets
Bitcoin (exposed keys)	Critical	P2PK addresses and reused P2PKH addresses have public keys on-chain; immediately stealable
Ethereum / Solana	Critical	Validator keys can be derived; enables consensus manipulation
DeFi protocols & bridges	High	Inherit vulnerabilities from underlying blockchains
Privacy features	High	All historical privacy guarantees become void retroactively

Special Risks: History Rewriting and Privacy Loss

Long-Range Attacks on Proof-of-Stake Chains

Proof-of-stake and Byzantine Fault Tolerant (BFT) consensus mechanisms face a unique vulnerability. Every block signed by a validator is permanently recorded on-chain. A quantum computer could derive the private keys of all historical validators from this public data and construct an alternative blockchain history that appears completely valid but contains different transactions [1].

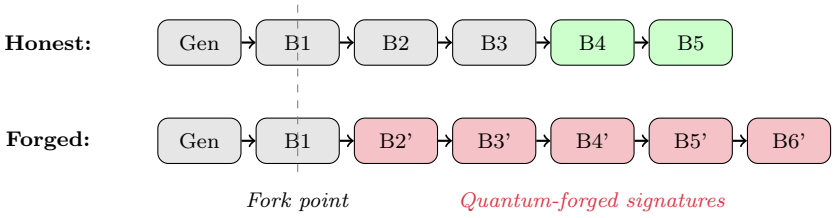

Figure 3: History rewriting attack: a quantum adversary derives historical validator keys and constructs an alternative chain with valid signatures.

Current defenses rely primarily on social mechanisms like trusted checkpoints and community consensus, which are insufficient in practice. A user returning after being offline cannot reliably distinguish the honest chain from a forged one when both contain cryptographically valid signatures. This represents a fundamental challenge to the long-term security model of proof-of-stake systems.

Retroactive Privacy Loss

Privacy loss is retroactive and permanent. While fund theft is a forward-looking risk (i.e., users who migrate to quantum-safe addresses beforehand are protected), privacy works differently. Every transaction is stored permanently on-chain, even on privacy-focused systems.[1] When quantum computers break the underlying cryptography, all historical transactions become visible on-chain. Once unhidden, there is no way to re-protect data which already has been recorded on public blockchains.

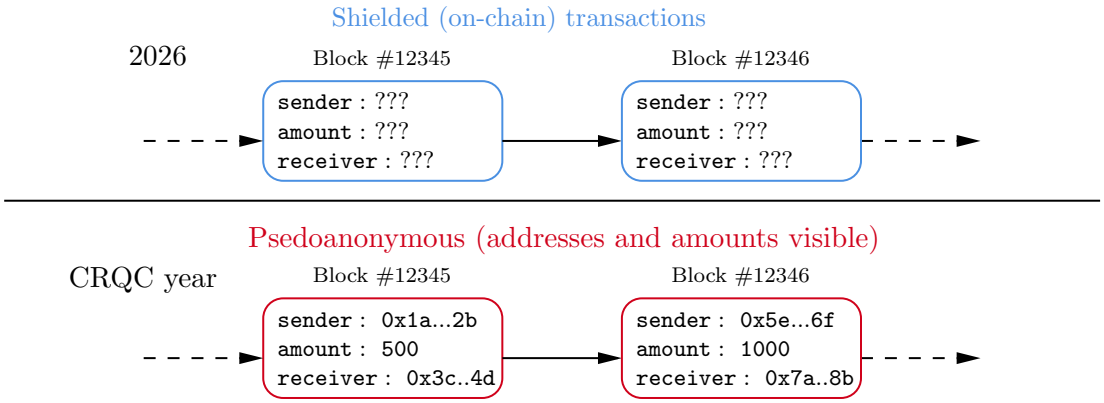

Figure 4: Transaction is encrypted today, but can be decrypted by a quantum attacker in the year when a Cryptographically Relevant Quantum Computer (CRQC) becomes available.

Proof-of-Work Mining Considerations

Proof-of-work mining faces a different category of threat. While Grover's algorithm cannot break hash functions outright, it could theoretically provide speedup for mining operations. Quantum-equipped miners might gain competitive advantages over classical miners, potentially destabilizing the economic balance that secures proof-of-work chains. The extent of this advantage remains an open research question, dependent on hardware realities, algorithm overhead, and how quickly difficulty adjustments respond. If the threat materializes, one potential mitigation is increasing hash output length (e.g., migrating from SHA-256 to SHA-512) to restore security margins, though this would require a coordinated protocol upgrade.

Assessing the Timeline: When Will the Quantum Era Arrive?

When will these threats materialize? The honest answer is that significant uncertainty remains. Today's best estimates suggest that breaking RSA-2048 requires approximately 1 million physical qubits [3], roughly $10,000$ times more than current machines, which operate with around 100 noisy physical qubits [4].

Timeline estimates vary widely depending on assumptions. At Google's current pace of hardware improvement (45% increase in qubit count every two years), some research models project

[1] This is distinct from the "harvest now, decrypt later" threat model commonly discussed in post-quantum literature, where an adversary must actively intercept and store encrypted network traffic. On blockchains, encrypted transaction data is already stored on-chain as an inherent part of the protocol state – the adversary need only download the publicly available ledger, requiring no special collection infrastructure.

RSA-2048 would not fall until 2076. If quantum hardware follows a Moore's-law trajectory (i.e., doubling every 18 months) the timeline compresses to 2046. Germany's Federal Office for Information Security (BSI) projects cryptographically relevant quantum computers could emerge as soon as 2040 [2].

Inconsistencies in defining "logical qubits". Industry announcements often count any encoded qubit as "logical," even those using codes that cannot scale to cryptographic applications. The logical qubits required for Shor's algorithm must be fully error-corrected and capable of executing complex non-Clifford gate operations (T-gates)—a far higher bar than current demonstrations. Surface codes, the most practical error-correction approach today, require roughly 1,000 physical qubits per logical qubit.

Factors That Could Accelerate the Quantum Timeline

Four categories of advancement could significantly accelerate these timelines:

- **Hardware breakthroughs** that improve qubit quality or reduce error rates
- **More efficient error-correcting codes** that reduce the physical-to-logical qubit ratio
- **Improved quantum algorithms** like Regev's new factoring approach that require fewer resources
- **Better circuit implementations** that optimize how quantum operations are executed

Recent expert assessments suggest cryptographic security may be easier to break than current estimates indicate. The field should expect unexpected developments that could shift timelines.

This uncertainty is precisely why organizations start preparations early. Blockchain protocol upgrades take years to design, test, and deploy across decentralized networks, for instance, Ethereum's transition to proof-of-stake required over five years. Organizations that wait for confirmation that cryptographically relevant quantum computers exist may not have time to migrate safely.

Key Considerations for Preparation

Preparing for the quantum era is not about predicting exactly when powerful quantum computers will arrive. It's about reducing risk now, so the transition is manageable whenever it happens. The research community has identified several areas that are commonly discussed as early considerations for the blockchain ecosystem.

1. **Cryptographic Dependencies** Blockchains, wallets, exchanges, and stablecoin issuers are often cited as needing to understand where vulnerable signature schemes are used and which cryptographic keys are exposed on-chain. Comprehensive auditing of these dependencies is essential as organizations cannot protect systems they have not fully inventoried.
2. **Better Key Management Practices** Simple operational changes can significantly reduce quantum attack surface. Avoiding address reuse, for example, prevents public keys from being exposed on-chain, making quantum attacks substantially harder. Improved key management practices are frequently discussed as a way to reduce quantum attack surface, particularly in scenarios where public keys are exposed on-chain. become pressing.

3. **Quantum-Safe Cryptography at System Edges** Systems such as node-to-node encryption, API authentication, and custodial infrastructure are often discussed as candidates for early experimentation with quantum-safe cryptographic primitives, since they operate independently of core consensus protocols. These components operate independently of core blockchain protocols and can be potentially upgraded without waiting for network-wide consensus upgrades.

4. **Core Protocol Upgrade Paths** Blockchain developers and researchers can design and test quantum-safe signature schemes, zero-knowledge proof systems, and consensus mechanisms so they are production-ready when protocols begin formal migration. This ensures that quantum-safe alternatives have been thoroughly vetted and can be deployed confidently when needed.

5. **Stablecoin Upgrades** Stablecoin issuers have a unique advantage: they can move faster than underlying blockchain protocols. Because stablecoins rely on off-chain governance keys and centralized issuance mechanisms, issuers can adopt quantum-safe signing systems now, long before the blockchains they operate on complete full migrations. While issuers can enhance their own signing systems, they remain subject to the underlying security and finality risks of the host blockchain. This independent action can protect the most concentrated value in the ecosystem years ahead of network-wide transitions.

These steps do not solve the entire quantum challenge, but they dramatically reduce long-term risk and ensure that when quantum computers do become relevant, the ecosystem will be ready to respond effectively.

Why Quantum-Safe Migration Takes Years

Transitioning blockchains to quantum-safe cryptography is not as straightforward as deploying a software update. It requires coordinated changes across an entire global ecosystem of independent actors and systems.

Ecosystem Complexity A single blockchain network depends on thousands of independent node operators, dozens of wallet providers, hardware manufacturers, exchanges, custodians, smart contract platforms, and in the case of stablecoins, regulated financial institutions. All these systems must upgrade in compatible ways without breaking existing applications or causing user fund losses.

Historical precedent demonstrates the timeline involved: major blockchain upgrades typically require years of design, security auditing, testing, community coordination, and gradual adoption. Even after new cryptography becomes available, the migration process involves multiple sequential steps:

- Wallet providers and custodians must update software to support new cryptographic primitives
- Users must actively move funds from old addresses to new quantum-safe addresses
- Smart contracts must be rewritten or migrated to use new signature schemes
- Cross-chain bridges and interoperability protocols must be upgraded simultaneously

Technical and Economic Costs Quantum-safe cryptography introduces real engineering tradeoffs. Post-quantum signatures are typically larger than current signatures, verification is computationally more intensive, and smart contracts may require architectural redesign. On high-throughput

blockchains, these overhead costs directly affect transaction fees, block sizes, and overall network performance.

Given this, research discussions often suggest modular migration models in which different components of the ecosystem transition independently and incrementally. This modular migration strategy strengthens security while helping participants to manage costs over time.

Governance and Coordination Challenges Blockchains operate through decentralized governance, which means protocol changes require broad consensus among stakeholders with diverse incentives. A migration of this scale across the global blockchain ecosystem is a considerably significant coordination challenge for the industry.

The Path Forward

Given the wide range of timeline estimates, many researchers argue that early analysis and preparedness discussions are warranted, even amid significant uncertainty. Blockchain protocol upgrades require years of design, testing, and coordination—waiting for certainty could mean limited time for effecting important changes.

While NIST and other standard organizations work to standardize key techniques and approaches, organizations can consider adopting upgrades that are not yet standardized. For instance, NIST has standardized post-quantum algorithms for basic signatures (ML-DSA, SLH-DSA) and key exchange (ML-KEM), but blockchains rely on primitives that NIST does not cover: non-interactive zero-knowledge proofs, ring signatures, verifiable random functions, and threshold signatures. Moreover, the blockchain community has historically favored algorithms outside NIST's selections, e.g., Bitcoin and Ethereum use secp256k1, which was not NIST standards. Quantum-safe blockchain cryptography will likely follow a similar path, driven by the specific needs of decentralized systems rather than government standardization timelines.

The blockchain industry, including organizations like Visa, is exploring post-quantum protocols tailored to payment systems. Research is ongoing to develop solutions that address blockchain-specific requirements beyond general-purpose NIST standards, with particular attention to stablecoin security given its systemic importance.

Migration also carries real engineering costs: quantum-safe signatures are larger, verification is slower, and smart contracts may need redesign. On high-throughput blockchains, these overheads affect transaction fees, block sizes, and performance. Given this, the modular approaches offer a viable path for protocols, wallets, and stablecoin issuers to adopt quantum-safe components strengthening security and managing migration costs.

For More Information

To learn more about Visa's quantum computing research or discuss quantum-safe solutions for stablecoins and digital payments, please contact:

Visa Crypto Team: gdlcryptoapp@visa.com

Limitations and Scope

This report focuses on cryptographic vulnerabilities in blockchain systems. It does not address:

- Specific product recommendations or implementations for any particular blockchain
- Investment advice or security guarantees
- Complete risk assessment for all quantum computing threats
- Regulatory compliance guidance for specific jurisdictions
- Timeline guarantees for quantum computing development

Readers should consult with qualified professionals for specific technical, legal, or financial advice. The analysis presented represents the research team's current understanding based on publicly available information and may require updating as quantum computing technology advances.

References

[1] Sarah Azouvi, Christian Cachin, Duc V. Le, Marko Vukolić, and Luca Zanolini. Modeling Resources in Permissionless Longest-Chain Total-Order Broadcast. In Eshcar Hillel, Roberto Palmieri, and Etienne Rivière, editors, *26th International Conference on Principles of Distributed Systems (OPODIS 2022)*, volume 253 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 19:1–19:23, Dagstuhl, Germany, 2023. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[2] Federal Office for Information Security (BSI). Aktualisierung der studie 'entwicklungsstand quantencomputer', 2025. Available at: `https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Aktualisierung_Studie_Quantencomputer_251219.html`.

[3] Craig Gidney. How to factor 2048 bit rsa integers with less than a million noisy qubits, 2025.

[4] Samuel Jaques. Expected and unexpected developments in quantum computing, 2025. Invited talk at PQCrypto 2025. Available at: `https://pqcrypto2025.iis.sinica.edu.tw/slides/Invited3.pdf`.

[5] Visa Onchain Analytics. Stablecoin supply dashboard, 2026. Accessed January 2026. Available at: `https://visaonchainanalytics.com/supply`.