Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 3, Issue 7, 2025

QUANTUM COMPUTING AND BLOCKCHAIN SECURITY: A CRITICAL ASSESSMENT OF CRYPTOGRAPHIC VULNERABILITIES AND POST-QUANTUM MIGRATION STRATEGIES

Mati Ullah[*1], Amjad Ali[2], Atif Khan Jadoon[3]

[*1,2]*Lahore School of Accountancy and Finance, University of Lahore, Pakistan*
[3]*Department of Economics, University of the Punjab, Pakistan*

DOI: https://doi.org/10.5281/zenodo.15844771

Keywords
Quantum Computing, Blockchain Security, Post-Quantum Cryptography, Shor's Algorithm, Grover's Algorithm, Cryptographic Vulnerability

Article History
Received: 02 April, 2025
Accepted: 23 June, 2025
Published: 09 July, 2025

Corresponding Author: *
Mati Ullah

Abstract
This paper examines the growing threat that quantum computing presents to blockchain security. Core blockchain cryptographic frameworks, specifically the Elliptic Curve Digital Signature Algorithm and the Secure Hash Algorithm 256, are vulnerable to quantum algorithms. Both the Shor algorithm and the Grover algorithm are capable of breaking the Elliptic Curve Digital Signature Algorithm, enabling attackers to calculate private keys from public keys, while the Grover algorithm can also compromise hash-based systems that depend on brute-force methods, such as Proof-of-Work. On-chain analysis indicates that billions of dollars' worth of crypto-assets are held in addresses susceptible to these quantum attacks. A proposed countermeasure is migration to Post-Quantum Cryptography, which incorporates quantum-resistant algorithms, such as CRYSTALS-Dilithium and Falcon. However, this migration introduces a trilemma among network security, decentralization, and performance. Post-Quantum Cryptography algorithms significantly increase transaction sizes and computational costs, which pose economic and technical challenges for large blockchain networks. The paper further discusses how the timeline for quantum advancements will be shaped by geopolitical competition, and how the catch-the-crop, decrypt-later strategy puts current data at risk from future quantum decryption. It emphasizes that active migration to Post-Quantum Cryptography is urgent, calling on stakeholders to prioritize system audits, transition to cryptographically flexible infrastructures, promote research into quantum-resistant solutions, and establish governance frameworks that enable prompt and decentralized upgrades.

INTRODUCTION

The present paper contends that the quantum threat to blockchain technology is multifaceted, urgent, and complex. This issue extends beyond a mere technical vulnerability, representing an institutional challenge that impacts network integrity, user trust, economic stability, and governance. A viable path to resilience lies in adopting Post-Quantum Cryptography, which consists of new classical cryptographic algorithms that are resistant to quantum attacks. However, integrating Post-Quantum Cryptography presents significant difficulties. The adoption of these algorithms introduces trade-offs regarding transaction size, computational requirements, associated costs, scalability, and increased governance complexity. This study finds that a trilemma exists at the center of Post-Quantum Cryptography migration: achieving robust quantum-resistant security, maintaining optimal network performance, and preserving decentralized

governance. Addressing this trilemma is crucial for safeguarding the blockchain ecosystem in the quantum era (Kumar and Pattnaik, 2020).

1.1. The Converging Revolutions of Blockchain and Quantum Computing

The twenty-first century has seen the simultaneous emergence of two transformative technologies: blockchain and quantum computing (Mosteanu and Faccia, 2021). Blockchain, first introduced with Bitcoin, revolutionized digital trust by enabling secure, transparent, and decentralized exchanges of value. This system eliminates the need for intermediaries such as banks or governments by relying on a distributed ledger, consensus mechanisms, and cryptographic protocols to validate transactions (Zaghloul et al., 2020; Kodithuwak & Pacillo, 2025). Such architecture enhances resistance to censorship and single points of failure, and its applications now extend beyond cryptocurrencies to areas like supply chain management and identity verification.

At the same time, as described by Tyagi and colleagues (2024), quantum computing has moved beyond the realm of science fiction and is advancing into experimental applications. Unlike classical computers, which process information using bits valued at zero or one, quantum computers utilize quantum bits, or qubits, that leverage superposition and entanglement to represent multiple states simultaneously. This capability for quantum parallelism allows for exponential improvements in computational power, enabling solutions to previously unsolvable problems in fields such as drug discovery, materials science, and complex optimization (Kulkarni et al., 2022; Minella, 2025).

1.2. The Cryptographic Collision

Although blockchain and quantum computing serve different purposes, their trajectories intersect critically in the realm of cryptographic security (Fernandez-Carames and Fraga-Lamas, 2020). Blockchain systems depend on asymmetric encryption, such as the Elliptic Curve Digital Signature Algorithm, and hash functions, such as Secure Hash Algorithm 256, which are based on mathematical problems considered intractable for classical computers. However, quantum algorithms such as the Shor algorithm and Grover algorithm challenge these assumptions. The Elliptic Curve Discrete Logarithm Problem, for example, can be efficiently solved using the Shor algorithm, thereby compromising public-key cryptography, while the Grover algorithm can significantly weaken hash-based protections and undermine consensus mechanisms such as Proof-of-Work (Larasati and Kim, 2021).

This convergence presents a fundamental threat to the security model on which blockchain technology is based. If fault-tolerant quantum computers become practical, current blockchain protocols may become obsolete—a point often referred to as Q-Day (Raheman, 2024). The question is no longer whether quantum capabilities will emerge, but rather when they will arrive. This represents a major systemic risk, especially as blockchain networks store trillions of dollars in digital assets and are increasingly integrated with the global financial infrastructure.

2. Literature Review

To understand the impact of quantum computing on blockchain security, it is essential to examine the foundational principles of both technologies. This section outlines the key concepts in quantum computing and blockchain architecture, with particular focus on the Shor algorithm and Grover algorithm, which represent significant threats to current cryptographic systems (Kumar et al., 2023). Additionally, it introduces Post-Quantum Cryptography, a promising category of cryptographic algorithms that remain resistant to known quantum attacks.

2.1. Principles of Quantum Computation

Quantum computing is based on the principles of quantum mechanics, rather than those of classical computing. Whereas classical bits can exist only in the states of zero or one, quantum bits, also known as qubits, can exist in multiple states simultaneously through a phenomenon called superposition (Swayne, 2024; Farras et al., 2025). This capability allows quantum computers to evaluate numerous possibilities in parallel, dramatically increasing computational power for certain types of problems.

Quantum computing relies on two fundamental properties: superposition and entanglement. Superposition permits each qubit to represent both

zero and one at the same time. Entanglement links qubits so that the state of one qubit can instantaneously influence the state of another, even across vast distances (Giovanni, 2024). When effectively utilized, these properties enable quantum computers to perform computations that would require classical computers millennia to complete.

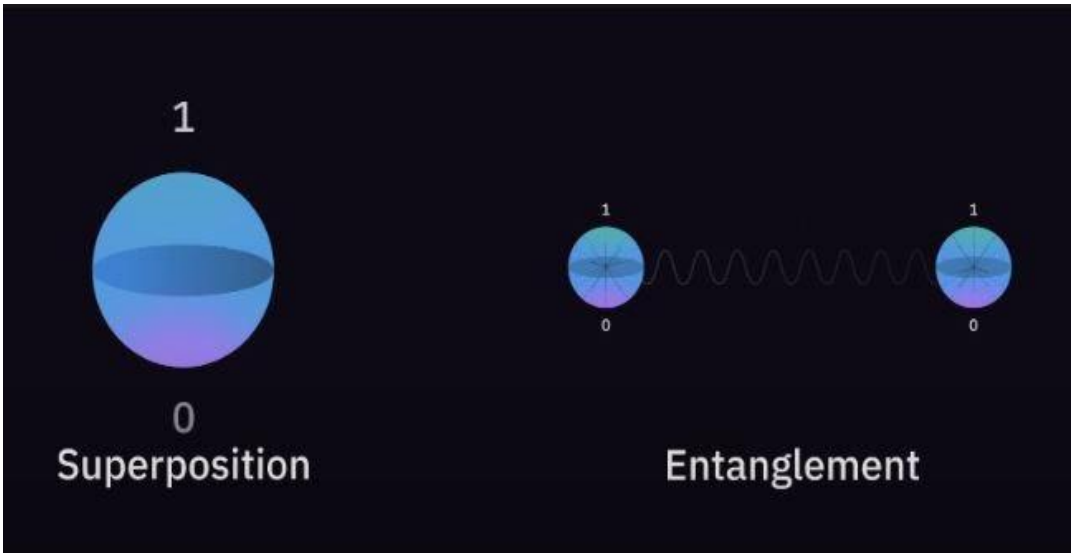

Figure 1: Superposition vs Entanglement [Source: (Singh, 2023)]

According to Martinez (2022), quantum interference is another important concept that quantum algorithms employ to amplify correct results and suppress errors. When the final state of a quantum algorithm is measured, the quantum state collapses into a classical value. This process introduces challenges such as decoherence, where external interactions degrade qubit states before they can be used for computation. Decoherence presents significant engineering hurdles to achieving stable and reliable quantum computation.

2.2. The Architectural Pillars of Blockchain Technology

Blockchain technology enables trust without centralized authority through the use of a distributed ledger and cryptography. The essential components are as follows (Paul et al., 2021):

Distributed Ledgers: A blockchain is maintained across a network of computers, ensuring that no single party controls the ledger. This decentralization enhances resistance to censorship.

Cryptographic Hashing (Secure Hash Algorithm 256): The Secure Hash Algorithm 256 cryptographic hash function secures the links between blocks and verifies data integrity, assuming classical computational limitations (Reddy et al., 2021; Shaukat et al., 2025).

Elliptic Curve Digital Signature Algorithm: The Elliptic Curve Digital Signature Algorithm verifies asset and transaction ownership. It is based on the mathematical difficulty of the elliptic curve discrete logarithm problem, which quantum computers can efficiently solve (Farooq et al., 2019).

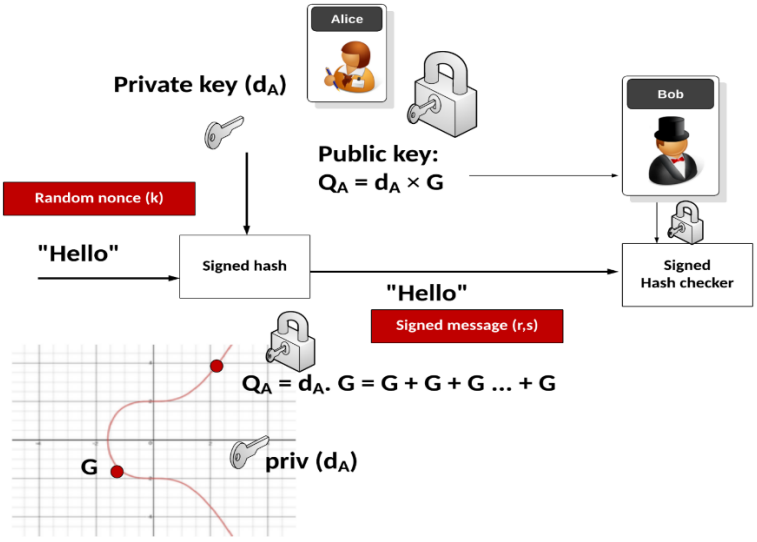

Figure 2: Elliptic Curve Digital Signature Algorithm (Security Site, 2025)

This image demonstrates the operation of the Elliptic Curve Digital Signature Algorithm, where a private key and a random nonce are used to produce a signed hash of a message (for example, "Hello"). The recipient verifies this signature using the corresponding public key, which is derived by multiplying the private key by a generator point. The security of this process is based on the computational difficulty of the elliptic curve discrete logarithm problem, a challenge that quantum computers could efficiently solve using the Shor algorithm. The combination of hashing and public key cryptography is fundamental to blockchain's immutable and trustless design.

2.3. The Quantum Arsenal

Two primary algorithms, namely the Shor algorithm and Grover algorithm, threaten the cryptographic foundations of blockchain due to their potential implementation on quantum computers (Yalamuri et al., 2022). These quantum algorithms challenge the assumption that certain mathematical problems are computationally infeasible to solve.

2.3.1. Shor's Algorithm

Shor's algorithm, developed by Peter Shor in 1994, provides an exponential speedup for factoring large integers and solving discrete logarithm problems. These tasks are impractical for classical computers, but quantum computers using the Shor algorithm can solve them in polynomial time. This capability poses a serious threat to public-key cryptography. Blockchain systems rely on the Elliptic Curve Digital Signature Algorithm, which assumes the elliptic curve discrete logarithm problem is infeasible to solve (Iqbal and Zafar, 2024; Reich & Reich, 2025). Shor's algorithm enables the extraction of private keys from public keys revealed during transactions. Once an attacker obtains a private key, they can sign fraudulent transactions and seize the associated funds (Wong, 2023). This vulnerability is present in most existing blockchain protocols because public keys are exposed on-chain during transaction validation.

2.3.2. Grover's Algorithm

In 1996, the Grover algorithm was introduced, providing a quadratic improvement in the time required to search unsorted databases or solve problems using brute force. While its impact on symmetric cryptography is significant, it is less transformative than the Shor algorithm. Grover's algorithm effectively reduces the security level of algorithms such as Secure Hash Algorithm 256 by half (Qiu et al., 2024). For instance, breaking a 256-bit hash function would require 2^128 operations with the Grover algorithm, which, while still substantial, is far more attainable than 2^256. Within blockchain systems, the Grover algorithm presents two primary threats:

Hash Function Weakening: Grover's algorithm weakens hash functions like Secure Hash Algorithm 256, making it easier to find matching preimages, threatening data integrity, and undermining block immutability.

Proof-of-Work Exploitation: Mining involves searching for a nonce that produces a hash meeting the network's difficulty criteria. According to Bailey and Sattath (2024), a quantum miner using the Grover algorithm could perform this task much more efficiently than a classical miner, leading to an unfair advantage and increasing the risk of a fifty-one percent attack.

2.4. The Countermeasure: An Overview of Post-Quantum Cryptography (PQC)

Due to the risks posed by quantum computers, the cryptographic community has developed Post-Quantum Cryptography, a set of algorithms designed to resist attacks from both conventional and quantum computers (Dam et al., 2023). These systems operate on traditional hardware but rely on mathematical problems that remain difficult to solve, even for quantum computers.

2.4.1. The NIST PQC Standardization Process

Recognizing the quantum threat, the United States National Institute of Standards and Technology initiated an international competition in 2016 to standardize Post-Quantum Cryptography algorithms. Following extensive testing and peer review, the first set of standards was released in 2024 (Valenta et al., 2024). The selected digital signature schemes are as follows:

CRYSTALS-Dilithium: A lattice-based scheme that provides strong security with relatively efficient performance.

Falcon: Another lattice-based algorithm noted for its small signature sizes and rapid verification.

SPHINCS+: A hash-based scheme that delivers conservative security assurances.

For key encapsulation, CRYSTALS-Kyber was chosen as the primary solution. These standards establish a foundation for upgrading key systems, including blockchains, to become resilient against quantum attacks.

2.4.2. Major Families of PQC

The algorithms selected and recommended by the United States National Institute of Standards and Technology fall into several primary categories:

Lattice-Based Cryptography: This widely supported family relies on complex problems such as Learning With Errors. Both Dilithium and Falcon algorithms belong to this category (Dam et al., 2023).

Code-Based Cryptography: Based on the difficulty of decoding certain codes, with McEliece as a well-known example. While considered secure, it involves large key sizes.

Hash-Based Signatures: Known for their conservative design and transparency. SPHINCS+ is in this category, providing robust security but at the cost of large signature sizes and slower signing speeds.

Multivariate Cryptography: Utilizes the challenge of solving systems of polynomial equations, offering small signatures but requiring large public keys.

Isogeny-Based Cryptography: Originally viewed as a promising approach to limit algorithm proliferation, its viability was questioned in 2022 when the SIKE protocol was compromised using a classical algorithm (Goodin, 2022), illustrating the immaturity and risk in some quantum-era proposals.

This overview underscores that quantum computing fundamentally threatens the cryptographic infrastructure underpinning blockchain systems. Shor and Grover algorithms expose significant vulnerabilities in digital signatures and hashing. While Post-Quantum Cryptography offers practical countermeasures, it also introduces a new balance between efficiency and complexity. The following section of the paper will address specific attack vectors, asset-risk quantification, and examine practical challenges in deploying Post-Quantum Cryptography within blockchain environments.

3. Methodology

This section outlines the qualitative research design developed to investigate the potential impact of quantum computing on blockchain security. The approach integrates theoretical modeling, evaluations by recognized experts, and detailed analysis of public blockchain data to assess the practicality and significance of adopting Post-Quantum Cryptography in real-world applications.

3.1. Research Design

The study employs an exploratory qualitative approach to identify emerging risks and potential countermeasures at the rapidly evolving intersection of quantum computing and blockchain technology (LÖSCH et al., 2023). Given the swift development in this field and the current scarcity of operational Post-Quantum Cryptography-based blockchains, the research team adopted a primarily conceptual, model-driven methodology rather than collecting new empirical data.

3.2. Data Collection Sources

The primary sources of information for this study included peer-reviewed journal articles, major standards such as the United States National Institute of Standards and Technology's Post-Quantum Cryptography papers, and reports or white papers from reputable organizations such as Deloitte, the International Monetary Fund, and blockchain analytics firms. Supplementary data were publicly available on-chain records from Bitcoin and Ethereum, which were analyzed to estimate the amount of digital assets potentially vulnerable to future quantum attacks.

All sources were evaluated based on publication authority, direct relevance to quantum computing and blockchain topics, and the technical rigor of the work, ensuring that only highly regarded documents contributed to the final models (Aspers and Corte, 2019).

4. Theoretical Model and Data Analysis

While the potential risk that quantum computing poses to blockchain systems is generally recognized, translating this risk into quantifiable and actionable insights is essential for developing an effective strategy (Baseri et al., 2025). This section simulates two primary quantum attack vectors, estimates the value of resources at risk within major blockchain networks, and examines the operational challenges involved in implementing Post-Quantum Cryptography.

4.1. Threat Vector Modeling

Quantum computing presents two major threats to blockchain systems: attacks on digital signatures using the Shor algorithm, and threats to consensus and hash security through the Grover algorithm (Preston, 2023).

Shor Algorithm Attack on Elliptic Curve Digital Signature Algorithm (Model 1): The Elliptic Curve Digital Signature Algorithm, widely used in blockchain, faces an existential threat from quantum computers running the Shor algorithm. In standard transactions, public keys are exposed when funds are spent. A quantum-capable adversary can extract this public key and use the Shor algorithm to compute the corresponding private key (Aranha et al., 2020). With the private key, the attacker can forge valid signatures, initiate unauthorized transactions, and seize control of the assets. This vulnerability is particularly severe for addresses that are reused or for funds that remain unspent after a transaction.

Grover Algorithm Attack on Proof-of-Work and Hashing (Model 2): The Grover algorithm weakens the Proof-of-Work mining mechanism by providing a quadratic speedup in searching for the correct nonce (Preston, 2023). Quantum miners gain an advantage by traversing the hash space more efficiently, leading to disproportionate influence over block creation. If a quantum miner controls fifty-one percent of the network's hash power, they could execute double-spending attacks, disrupt transactions, or destabilize network consensus. Additionally, Grover's algorithm reduces the effective pre-image resistance of Secure Hash Algorithm 256 to 2^128 operations, which weakens the security foundation of block immutability (Schärer and Comuzzi, 2023).

4.2. Analysis of the Vulnerable Population

Analysis of public blockchain data shows that a significant portion of crypto-assets are already vulnerable to quantum attacks, due to the exposure of

public keys and the risk posed by the Shor algorithm (Zhou et al., 2024).

4.2.1. Exposure of Addresses of Bitcoins

Early Bitcoin addresses were created in the Pay-to-Public-Key format, where the full public key is embedded directly in the transaction output, leaving these funds fully exposed. The Pay-to-Public-Key-Hash format only reveals the public key when a transaction is made to spend funds. However, once the public key is exposed, any remaining balance at that address becomes vulnerable to quantum attacks (Melo et al., 2023).

According to an analysis by Deloitte, approximately four million Bitcoins, representing about one quarter of all Bitcoins in circulation, are stored in address formats that are susceptible to quantum attacks (Deloitte, 2025).

Table 1: Estimated Quantum-Vulnerable Bitcoin Holdings by Address Type

Address Type	Approx. BTC Vulnerable	% of Supply	Est. Value (USD)
P2PK	1.5 – 1.9 million	~9–10%	> $15 billion
Reused P2PKH	~2.5 million	~14–15%	> $25 billion
Total	~4 million	~25%	> $40 billion

Many of these addresses hold dormant or lost funds, such as those linked to Bitcoin creator Satoshi Nakamoto, which are unlikely to be moved to more secure address types and will remain persistent targets for future quantum attacks.

4.2.2. Cross-Cryptocurrency Extrapolation

Bitcoin is not the only cryptocurrency at risk. Ethereum and most major cryptocurrencies also rely on the Elliptic Curve Digital Signature Algorithm or other similarly vulnerable cryptographic systems. Given market capitalization and technological similarities, it is plausible that twenty to thirty percent of total cryptocurrency value, equivalent to tens of billions of dollars, could be at risk (Rankhambe and Khanuja, 2019). The International Monetary Fund and organizations such as BlackRock have identified the quantum threat as a systemic risk to digital financial systems.

4.3. Performance Modeling of PQC Integration

Although Post-Quantum Cryptography provides a form of defense, integrating these algorithms into blockchain protocols introduces significant trade-offs in performance and cost (Sami et al., 2024). The primary differences involve signature size, key size, and verification speed—factors that directly impact transaction cost, network throughput, and node storage requirements.

4.3.1. Performance Comparison of Key: ECDSA vs. PQC Candidates

The following list provides a summary of the Elliptic Curve Digital Signature Algorithm and two leading candidates for the United States National Institute of Standards and Technology Post-Quantum Cryptography digital signature standard, CRYSTALS-Dilithium and Falcon.

Table 2: Performance Comparison of ECDSA and NIST-Standardized PQC Signature Schemes

Algorithm	Security Level (NIST)	Public Key Size (Bytes)	Signature Size (Bytes)	Key Gen Time (ms)	Signing Time (ms)	Verification Time (ms)
ECDSA (secp256k1)	~128-bit (Pre-Quantum)	32 / 64	~71	~0.02	~0.04	~0.05 - 0.47
CRYSTALS-Dilithium2	1	1,312	2,420	~0.06	~0.13	~0.07
CRYSTALS-Dilithium3	3	1,952	3,293	~0.10	~0.24	~0.12
CRYSTALS-Dilithium5	5	2,592	4,595	~0.14	~0.34	~0.17
Falcon-512	1	897	666	~1.31	~3.28	~0.03
Falcon-1024	5	1,793	1,280	~4.70	~7.50	~0.06
SPHINCS+-SHA2-128s	1	32	7,856	~0.10	~131.93	~3.64

Dilithium signatures are 34 to 65 times larger than those produced by the Elliptic Curve Digital Signature Algorithm, while Falcon provides smaller signatures but with reduced signature speed and more complex key generation (Snetkov et al., 2024). Although these differences may appear minor individually, their impact becomes significant at scale.

4.3.2. On-Chain Implications

Larger signatures increase transaction sizes, which in turn consume more space within each block and contribute to blockchain bloat (Alzoubi and Mishra, 2024). This raises hardware and bandwidth requirements for operating a full node, potentially leading to greater network centralization over time.

The increased size of transactions results in slower propagation across the network, causing additional delays in block propagation and confirmation times.

Verifying Post-Quantum Cryptography signatures is more complex on smart contract platforms such as Ethereum, requiring greater gas payments to miners. Experiments with Dilithium in smart contracts show that a single Post-Quantum Cryptography signature verification can consume up to nine times more gas than an Elliptic Curve Digital Signature Algorithm signature (Marchsreiter, 2025). This significantly increases transaction costs and could hinder adoption unless scalability solutions are developed.

Quantum attacks on blockchain systems are no longer merely hypothetical—millions of coins, worth tens of billions of dollars, are already exposed to key-extraction attacks. Implementing quantum-safe cryptography, such as Dilithium or Falcon, is necessary but brings considerable performance challenges that blockchains must overcome to stay functional, decentralized, and economically viable. The next section will discuss the broader technological, geopolitical, and economic implications of these findings, as well as future governance and migration challenges.

5. Results and Discussion

The above examination measured the extent of the magnitude of the exposure of blockchain to quantum threats, and it highlighted the performance trade-offs associated with the implementation of Post-Quantum Cryptography (PQC) (Dam et al., 2023). This part relates those results to the wider real-world consequences, addressing schedules of fault-tolerant quantum computing, financial risk, suitability of PQC, and the problem of crypto migration governance. In combination, these factors expose a complicated and time-critical choice environment to blockchain environments facing an inexorable post-quantum shift.

5.1. The Horizon Q-day

The danger that quantum computing would pose to cryptography was viewed as remote over the years. Nevertheless, recent announcements and roadmaps of quantum research giants have reduced the timeframe to a cryptographically meaningful quantum computer (CRQC) to the near future, which has added new urgency (Raheman, 2024).

5.1.1. IBM's Roadmap

In 2025, IBM published its path to developing IBM Quantum Starling, a fault-tolerant quantum system that is expected to run by 2029 (Mandelbaum et al., 2025). The machine would likely have an estimated 200 logical qubits and could perform 100 million gate operations, which, it would be said, could break cryptographic systems such as ECDSA. The proposed timeline is not hypothetical-intermediate steps, such as Loon and Kookaburra processors, are under development to be able to perform scalable quantum error correction.

5.1.2. Pascal and Academic Research

With neutral-atom quantum processors, Pascal also plans to have hundreds of logical qubits by decade-end. In the meantime, an ongoing sequence of research advancements in the fields of organizations, such as MIT, in regard to quicker qubit operations, management overall, and readout effectiveness, have proceeded to narrow down the divide between noisy intermediate-scale quantum (NISQ) and fault-tolerant apparatus (Erata et al., 2023).

5.1.3. Geopolitical Drivers

International quantum research and development has surpassed the mark of $40 billion in investment and is driven mainly due to national preferences (Qureca, 2025). Countries such as the U.S. and China believe quantum supremacy is a critical economic, military, and cybersecurity leadership issue. It is a fast-tracking

arms race that risks a sudden, unheralded development, such as a potential, what might come to be known as a quantum Pearl Harbor, where cryptographic systems can be cracked without prior notice.

5.2. Financial Stability and the Quantum Domino Effect

The quantum threat is not only a technical one, but it also poses some systemic financial risks. The possibility of massive data decryption and blockchain intrusion may spread waves in the digital and conventional monetary markets.

5.2.1. Harvest Now, Decrypt Later (HNDL)

The strategy of HNDL is one of the most urgent threats. Because the public blockchains are immutable and public, the adversary can obtain historical blocks of transactions that expose some publicly known keys (Olutimehin et al., 2025). These keys may be reverse-engineered to generate private keys after a CRQC has been discovered, and in this way, an address that may seem inactive can be stolen by the Shor algorithm. This makes the quantum threat not to be future-tense, but present and cumulative.

5.2.2. Systemic Contagion

An effective assault on one of the largest currencies, such as Bitcoin, would cause more than the loss of assets. As previously stated in the analysis, approximately 25 percent or more than $40 billion of the supply of Bitcoin is stored in quantum-susceptible forms (AI Invest, 2025). In case such assets were to suddenly unravel and become liquidated, then it would create all-out anarchy in the marketplace; a meltdown in the price level, trust damage, and panic among the investors.

This would not end up in the crypto ecosystem. As the realms of traditional and crypto finance merge- especially in spot ETFs, institutional investment, and tokenized securities- the risk of a huge decline in crypto prices would lead to actual losses on pension funds, banks, and asset managers. As per Redo & Gębska (2020), the IMF has threatened that the resulting collapse of cryptography will likely render the world financial markets unstable, especially in case the quantum threats outpace the current security infrastructure responses.

5.3. Evaluating PQC for Blockchain Environments

Considering this emergency, it is necessary to migrate to PQC. Nonetheless, there should be a trade-off between security, performance, and the implementation possibility of the algorithm, particularly significant in blockchain, where bandwidth, latency, and cost are central questions.

Lattice-Based Candidates- Dilithium and Falcon: Among the standardized digital signature schemes at NIST, one can distinguish CMST-Dilithium and Falcon. Dilithium offers an acceptable balance between speed, ease, and implementation security. Dilithium is preferred for its balance of speed, simplicity, and implementation security. While its signatures are significantly larger than ECDSA's (~2.4 KB vs. ~71 bytes), its resistance to side-channel attacks and relatively straightforward design make it a practical candidate for many platforms (Beckwith et al., 2022).

Falcon, in its turn, provides the smallest signatures (~666 bytes) and verification speed, which is especially useful in that case when all nodes should be able to verify every transaction. It is, however, harder to use securely since it requires the use of low-precision arithmetic, and this can make it more prone to bugs and to side-channel attacks.

Hash-Based Alternative - SPHINCS+: The most conservative option is SPHINCS+, which only uses the security of a hash function instead of using a problem in number theory (Zhang et al., 2022). Its signature size (17 KB) is huge, and the signature generation is pathologically slow, but it is also an important fallback in the event security problems are found in the lattice-based schemes.

5.4. The Migration Trilemma: Security, Decentralization, Feasibility

PQC transition sets a trilemma upon blockchain ecosystems. All three of the following objectives go hand in hand; it is incredibly hard to achieve two of them at the same time (Paul et al., 2022):

1. Security: The transition to quantum-resistant cryptography.
2. Decentralization: Maintaining the decentralized, democratic, and consensus-based nature of blockchain governance.

3. Feasibility: Making the migration both technically and economically straightforward.

Bitcoin's Hardline Proposal – QRAMP: QRAMP (Quantum-Resistant Address Migration Protocol) is a hard fork proposal in Bitcoin on which users would have to migrate funds to quantum-safe key types or lose access. This puts emphasis on security, but it cuts on feasibility and decentralization (Baseri et al., 2025). A large number of users might become stranded, and a hard fork could destroy the community.

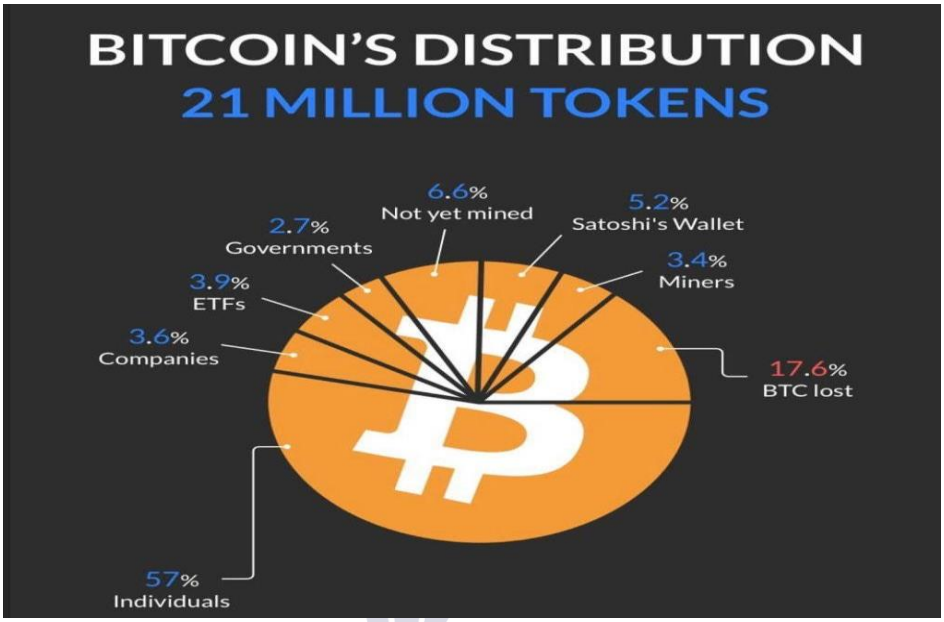

Figure 3: Bitcoin's 21-million limit survives quantum and cross-chain pressures (Andreou, 2025)

This image highlights the diverse distribution of Bitcoin ownership, revealing that a significant portion, such as the 57% held by individuals and 17.6% already lost, could face permanent loss or exclusion under QRAMP's hard fork mandate, raising serious concerns about the feasibility and inclusiveness of such a transition.

The Crypto-Agile Strategy of Ethereum: Ethereum is going toward a more modular structure. Rather than pursuing a hard fork, it is also considering crypto-agility, where components of a protocol (signatures, hashing, validator credentials) can be replaced over time (Alnahawi et al., 2023). Such features as account abstraction and opcode expansion of PQC will facilitate pathways to optional adoption to avoid distraction or even the loss of user choice.

As it becomes clear in the discussion, a threat to blockchain posed by quantum is not a far-future theory anymore; it is a fast-approaching reality. Recent developments by IBM and Pasqal, among other players, have reduced the gap to a matter of a few years before a CRQC becomes a reality. In the meantime, there are financial dangers of failure to act, in particular, by harvest-now, decrypt-later approaches, which over time could jeopardize trillions of dollars of digital assets and create large-scale financial market uncertainty.

PQC is a way out, but there is no universal solution. Lattice schemes, such as Dilithium and Falcon, are ideal on the trade-off between simple/fast and fast, and hash-based schemes such as SPHINCS+ offer conservative backup. However, there is a bigger challenge of governance that is beyond cryptographic engineering. Every large blockchain ecosystem has to take care of the PQC migration trilemma, picking and choosing among security, decentralization, and feasibility. It may be by means of hard forks, soft upgrades, or crypto-agile modularity - something is going to need to be done now. The more systems delay prioritizing the problem of the first real quantum attack, the more likely they can find themselves attacked by it and have the ledger overwritten, to boot.

6. Conclusion

The intersection of quantum computing and blockchain technology represents a significant and urgent threat to online security. Analysis in this study shows that the cryptographic foundations of blockchain, specifically the Elliptic Curve Digital Signature Algorithm and Secure Hash Algorithm 256, are directly vulnerable to quantum techniques such as the Shor algorithm and Grover algorithm. This is not a distant possibility-fault-tolerant quantum computers are now projected to arrive within the next three to five years, with accelerated development announced by companies like IBM and Pasqal. The quantum threat is not only real but is accelerating.

Currently, one in four Bitcoins-representing over forty billion dollars, is already at risk due to exposed public keys, and similar vulnerabilities exist across other major blockchains. The approach of capturing encrypted data now and decrypting it later means quantum computing could eventually compromise substantial amounts of digital assets. The systemic risk is broader than cryptocurrency alone, potentially destabilizing the global financial system as blockchain technology becomes more integrated with traditional finance.

While Post-Quantum Cryptography offers a pathway to resilience, its adoption comes at a cost to performance, decentralization, and usability. Post-Quantum Cryptography algorithms result in larger, more complex transactions, presenting new challenges for network scalability and user adoption. The transition to Post-Quantum Cryptography brings forth a trilemma, balancing these concerns with the complexities of decentralized governance.

6.1. Action Points

Blockchain developers and companies should begin cryptographic audits and conduct market testing for Post-Quantum Cryptography solutions. Delaying action until quantum systems are operational is no longer a viable option.

Protocols should be designed for future adaptability, allowing for seamless cryptographic updates. Hybrid schemes that combine classical and Post-Quantum Cryptography algorithms can provide transitional protection.

Engage with standardization bodies such as the United States National Institute of Standards and Technology and collaborate with open-source initiatives like the Open Quantum Safe and Post-Quantum Cryptography Coalition to develop robust and scalable Post-Quantum Cryptography tools.

Focus research efforts on the practical effectiveness of Post-Quantum Cryptography and establish governance frameworks that enable decentralized but timely responses to emerging security threats.

REFERENCES

AI Invest. (2025, June 3). Bitcoin faces imminent quantum threat with 25% supply vulnerable. AI Invest.

Alnahawi, N., Schmitt, N., Wiesmaier, A., Heinemann, A., & Grasmeyer, T. (2023). On the state of crypto-agility. Cryptology ePrint Archive.

Alzoubi, Y. I., & Mishra, A. (2024). Techniques to alleviate blockchain bloat: Potentials, challenges, and recommendations. Computers and Electrical Engineering, 116, 109216.

Andreou, G. (2025, June 8). QRAMP protocol, explained: Can Bitcoin's 21-million cap survive the future? Medium.

Aranha, D. F., Novaes, F. R., Takahashi, A., Tibouchi, M., & Yarom, Y. (2020). LadderLeak: Breaking ECDSA with less than one bit of nonce leakage. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (pp. 225–242).

Aspers, P., & Corte, U. (2019). What is qualitative in qualitative research. Qualitative Sociology, 42, 139–160.

Bailey, B., & Sattath, O. (2024). 51% attack via difficulty increase with a small quantum miner. arXiv preprint arXiv:2403.08023.

Baseri, Y., Hafid, A., Shahsavari, Y., Makrakis, D., & Khodaiemehr, H. (2025). Blockchain security risk assessment in quantum era, migration strategies and proactive defense. arXiv preprint arXiv:2501.11798.

Beckwith, L. N. (2022). High-performance hardware implementation of lattice-based digital signatures. Cryptology ePrint Archive.

Dam, D. T., Tran, T. H., Hoang, V. P., Pham, C. K., & Hoang, T. T. (2023). A survey of post-quantum cryptography: Start of a new race. Cryptography, 7(3), 40.

Deloitte. (2025, June 18). Quantum computers and the Bitcoin blockchain. Deloitte.

Erata, F., Piskac, R., Mateu, V., & Szefer, J. (2023). Towards automated detection of single-trace side-channel vulnerabilities in constant-time cryptographic code. In 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P) (pp. 687–706). IEEE.

Farooq, S. M., Hussain, S. S., & Ustun, T. S. (2019). Elliptic curve digital signature algorithm (ECDSA) certificate-based authentication scheme for advanced metering infrastructure. In 2019 Innovations in Power and Advanced Computing Technologies (i-PACT) (Vol. 1, pp. 1–6). IEEE.

Farras, A., Ali, A., & Audi, M. (2025). Advancing Audit Practices through Technology: A Comprehensive Review of Continuous Auditing. Journal of Social Signs Review, 3(2), 506-539.

Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE Access, 8, 21091–21116.

Giovanni, F. D. (2024, January 5). Physical principles underpinning quantum computing. ET Times.

Goodin, D. (2022, August 3). A new attack easily knocked out a potential encryption algorithm. Wired.

Iqbal, S. S., & Zafar, A. (2024). Enhanced Shor's algorithm with quantum circuit optimization. International Journal of Information Technology, 16(4), 2725–2731.

Kodithuwak, S., & Pacillo, N. (2025). Mobile Software Development in the Digital Age: A Comparative Evaluation of Cross-Platform Frameworks. Journal of Policy Options, 8(2), 9-17.

Kulkarni, A. U., Jain, S., & Kumar, A. (2022). Quantum computing and quantum blockchain: Recent advancements, analysis and future directions. In Quantum and Blockchain for Modern Computing Systems: Vision and Advancements (pp. 311–339). Springer International Publishing.

Kumar, D. K., Krishna, E. H. V., Ushasri, R., Jahnavi, V., Prakash, K. B., & Imambi, S. (2023). Implementation of Grover's and Shor's algorithms in quantum machine learning. In 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE) (pp. 967–972). IEEE.

Kumar, M., & Pattnaik, P. (2020). Post quantum cryptography (PQC)–an overview. In 2020 IEEE High Performance Extreme Computing Conference (HPEC) (pp. 1–9). IEEE.

Larasati, H. T., & Kim, H. (2021). Quantum cryptanalysis landscape of Shor's algorithm for elliptic curve discrete logarithm problem. In Information Security Applications: 22nd International Conference, WISA 2021 (pp. 91–104).

Lösch, S., Rambo, C. A., & de Lima Ferreira, J. (2023). Exploratory research in the qualitative approach in education. Revista Ibero-Americana de Estudos Em Educação, 18.

Mandelbaum, R., Gambetta, J., Chow, J., Mittal, T., Yoder, T. J., Cross, A., & Steffen, M. (2025, June 10). How IBM will build the world's first large-scale, fault-tolerant quantum computer. IBM.

Marchsreiter, D. (2025). Towards quantum-safe blockchain: Exploration of PQC and public-key recovery on embedded systems. IET Blockchain, 5(1), e12094.

Martinez, J. E. (2022). Decoherence and quantum error correction for quantum computing and communications. arXiv preprint arXiv:2202.08600.

Melo, D., Hernandez, S. P., Rodríguez, L., & Pérez-Sansalvador, J. C. (2023). Bitcoin transactions types and their impact on storage scalability. In 2023 IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE) (pp. 1–6). IEEE.

Minella, C. (2025). Managing Agile Across Borders: A Review of Scrum Implementation in Globally Distributed Software Development. Journal of Policy Options, 8(2), 37-45.

Mosteanu, N. R., & Faccia, A. (2021). Fintech frontiers in quantum computing, fractals, and blockchain distributed ledger: Paradigm shifts and open innovation. Journal of Open Innovation: Technology, Market, and Complexity, 7(1), 19.

Olutimehin, A. T., Joseph, S., Ajayi, A. J., Metibemu, O. C., Balogun, A. Y., & Olaniyi, O. O. (2025). Future-proofing data: Assessing the feasibility of post-quantum cryptographic algorithms to mitigate 'harvest now, decrypt later' attacks. Decrypt Later' Attacks.

Paul, P., Aithal, P. S., Saavedra, R., & Ghosh, S. (2021). Blockchain technology and its types—A short review. International Journal of Applied Science and Engineering (IJASE), 9(2), 189–200.

Paul, S., Scheible, P., & Wiemer, F. (2022). Towards post-quantum security for cyber-physical systems: Integrating PQC into industrial M2M communication. Journal of Computer Security, 30(4), 623–653.

Preston, R. H. (2023). Applying Grover's algorithm to hash functions: A software perspective. IEEE Transactions on Quantum Engineering, 3, 1–10.

Qiu, D., Luo, L., & Xiao, L. (2024). Distributed Grover's algorithm. Theoretical Computer Science, 993, 114461.

Qureca. (2025, June 5). Quantum initiatives worldwide 2025. Qureca.

Raheman, F. (2024). Defining quantum advantage for building a sustainable MVP to deliver quantum computing services. Open Journal of Applied Sciences, 14(6), 1530–1549.

Raheman, F. (2024). Futureproofing blockchain & cryptocurrencies against growing vulnerabilities & Q-Day threat with quantum-safe ledger technology (QLT). Journal of Computer and Communications, 12(7), 59–77.

Rankhambe, B. P., & Khanuja, H. K. (2019). A comparative analysis of blockchain platforms—Bitcoin and Ethereum. In 2019 5th International Conference on Computing, Communication, Control and Automation (ICCUBEA) (pp. 1–7). IEEE.

Reddy, G. P., Narayana, A., Keerthan, P. K., Vineetha, B., & Honnavalli, P. (2021). Multiple hashing using SHA-256 and MD5. In Advances in Computing and Network Communications: Proceedings of CoCoNet 2020, Volume 1 (pp. 643–655). Springer Singapore.

Redo, M., & Gębska, M. (2020). Globalization in growing financial markets as a threat to the financial security of the global economy. European Research Studies Journal, 23(Special 1), 335–355.

Reich, A., & Reich, N. (2025). Scrum in Global Software Development: Challenges, Risks, and Mitigation Strategies for Effective Project Management. Journal of Policy Options, 8(1), 43-50.

Sami, M. S. U. I., Azar, K. Z., Kamali, H. M., Farahmandi, F., & Tehranipoor, M. (2024). PQC-HI: PQC-enabled chiplet authentication and key exchange in heterogeneous integration. In 2024 IEEE 74th Electronic Components and Technology Conference (ECTC) (pp. 464–471). IEEE.

Schärer, K., & Comuzzi, M. (2023). The quantum threat to blockchain: Summary and timeline analysis. Quantum Machine Intelligence, 5(1), 19.

Security Site. (2025, June 17). Elliptic curve digital signature algorithm (ECDSA). Security Site.

Shaukat, H., Ali, A., & Audi, M. (2025). Artificial Intelligence and Economic Transformation: Implications for Growth, Employment, and Policy in the Digital Age. Research Consortium Archive, 3(2), 852-869.

Singh, A. (2023, August 7). Unveiling quantum wonders: Superposition and entanglement in quantum computing. Medium.

Snetkov, N., Vakarjuk, J., & Laud, P. (2024). TOPCOAT: Towards practical two-party Crystals-Dilithium. Discover Computing, 27(1), 18.

Swayne, M. (2024, April 12). What is quantum computing? Quantum Insider.

Tyagi, A. K., Mishra, A. K., Aswathy, S. U., & Kumari, S. (2024). Quantum computing, qubits with artificial intelligence, and blockchain technologies: A roadmap for the future. In Automated Secure Computing for Next-Generation Systems (pp. 367–384).

Valenta, L., Gonçalves, V., & Westerbaan, B. (2024, August 20). NIST's first post-quantum standards. Cloudflare.

Wong, H. Y. (2023). Shor's algorithm. In Introduction to Quantum Computing: From a Layperson to a Programmer in 30 Steps (pp. 289–298). Springer International Publishing.

Yalamuri, G., Honnavalli, P., & Eswaran, S. (2022). A review of the present cryptographic arsenal to deal with post-quantum threats. Procedia Computer Science, 215, 834–845.

Zaghloul, E., Li, T., Mutka, M. W., & Ren, J. (2020). Bitcoin and blockchain: Security and privacy. IEEE Internet of Things Journal, 7(10), 10288–10313.

Zhang, K., Cui, H., & Yu, Y. (2022). SPHINCS-α: A compact stateless hash-based signature scheme. Cryptology ePrint Archive.

Zhou, Y., Chen, J., Wang, Y., Tang, Y., & Gu, G. (2024). Towards understanding crypto-asset risks on Ethereum caused by key leakage on the Internet. In Companion Proceedings of the ACM Web Conference 2024 (pp. 875–878)..