Sci

MDPI

Review

A Comprehensive Review of Quantum-Resistant Architectures for Blockchain Security

Hamed Taherdoost

College of Technology and Engineering, Westcliff University, Irvine, CA 92614, USA; hamed.taherdoost@gmail.com

Abstract

The nascent quantum computing brings unprecedented threats to the security roots of blockchain technology, potentially compromising cryptographic protocols securing decentralized systems. This review paper discusses the developing quantum threat scenario, focusing on the effect of quantum algorithms on traditional cryptographic systems. We critically examine current blockchain architectures, highlighting their vulnerabilities in a post-quantum future. The paper explores newer quantum-resistant cryptographic and modular architectural techniques to enhance blockchain resilience. This review supports comprehensive comprehension of cutting-edge strategies and research gaps by combining the literature addressing quantum threat modeling and post-quantum cryptography in decentralized systems.

Keywords: quantum-resistant cryptography; post-quantum blockchain; lattice-based signatures; hybrid cryptographic schemes; consensus re-engineering; blockchain migration strategies

1. Introduction

Blockchain technology is built on a decentralized ledger system, ensuring the integrity and security of data through cryptographic techniques. Consensus algorithms employed in blockchain protocols are essential to ensure the safety and efficacy of blockchain systems. The choice of consensus algorithms can play a crucial role in the operation of blockchain applications, and hence, well-established mechanisms should be selected to enhance security and effectiveness [1].

Blockchain security is also enhanced by its immutable nature, which will not permit unauthorized data modification in the ledger [2,3]. This aspect is particularly beneficial in sectors such as supply chain management, where traceability and transparency are the highest priority. Helo and Hao [4] point to how blockchain technology can be used in operations and supply chains and demonstrate how immutable ledgers can enhance transaction report reliability.

Blockchain technology is not free from vulnerabilities. Fraga-Lamas and Fernández-Caramés [5] emphasize the need for robust cybersecurity measures in the automotive industry, in which Blockchain can improve data protection and privacy. As a combination with other technologies such as IoT, blockchain has other security threats that must be addressed for these systems' development to be resilient [6]. Research studies have already begun analyzing these threats in an organized manner. Kearney and Pérez-Delgado [7] provide a vulnerability assessment of top cryptocurrencies, Bitcoin, Ethereum, Litecoin, and ZCash, quantifying exposure to quantum attacks and approximating quantum threat

Academic Editors: Carson K. Leung and Gerald B. Cleaver

Received: 15 October 2025
Revised: 10 December 2025
Accepted: 15 February 2026
Published: 19 February 2026

timetables. A survey by Khodaiemehr et al. [8] also scopes the threat to public-key schemes and hash functions in blockchains and discusses potential countermeasures. More recent literature also addresses the threat vectors (consensus, wallet security, signature schemes) and the requirement of quantum resilience in cryptographic design [9].

The advent of quantum computing introduces a new paradigm that threatens the cryptographic basis of blockchain technology. Quantum computers can execute algorithms like Shor's and Grover's that can compromise broadly deployed cryptographic systems, including those found in blockchain networks [10].

Developing secure blockchain architectures is essential to offset the threat posed by quantum computing. This involves incorporating post-quantum cryptographic techniques and developing robust consensus protocols immune to upcoming attacks. Gai et al. [11] mention the incorporation of Blockchain with cloud computing, pointing to the potential for better security and performance using distinctive architectural designs. Blockchain integration with upcoming technologies such as digital twins and IoT can contribute to creating more robust systems. Hemdan et al. [12] explain how digital twins can be integrated with Blockchain for data integrity protection in various applications. This may allow real-time asset monitoring and control, further strengthening the security position of blockchain networks.

Although such advancements are available, adapting blockchain ecosystems to quantum-resistant architectures remains in infancy. Challenges come in the form of large overheads (computation, bandwidth, and storage) that come with most PQC schemes; how they can be integrated into existing blockchain protocols and consensus algorithms; interoperability between classical and post-quantum components; and governance issues, such as how to make live upgrades without disrupting network operations. There are concerns about the timing when quantum computers will be "cryptographically relevant" (i.e., able to break widely used cryptographic schemes in practical scenarios), with implications for how rapidly the transition needs to occur [13].

The recent literature includes several surveys addressing blockchain security and post-quantum cryptography. These works differ in analytical focus, coverage of architectural issues, and treatment of migration pathways. Some studies emphasize cryptographic primitives, while others focus on consensus, system design, or attacker capabilities. Table 1 summarizes representative surveys and clarifies their scope relative to this work.

Table 1. Comparative summary of prior surveys on quantum-era blockchain security.

Survey	Year	Scope	Methodology	Key Conclusions
Kearney & Pérez-Delgado [7]	2021	Vulnerability of major cryptocurrencies	Quantitative exposure modeling	Estimates timelines for quantum risk
Fernandez-Caramés & Fraga-Lamas [10]	2020	PQC readiness of blockchain	Cryptographic/architectural review	Highlights need for cryptographic upgrades
Yang et al. [13]	2023	Comparison of quantum and post-quantum blockchains	Layer-based analysis	Discusses quantum-native vs. PQC-enhanced systems
Khodaiemehr et al. [8]	2023	Threats to public-key and hash systems in blockchain	Structured threat mapping	Provides countermeasures and technical considerations
This Review	2025	Quantum-resistant architectures and migration design	Architecture-centric synthesis	Emphasizes modularity, migration frameworks, and system-level resilience

This survey aims to distill current understanding about quantum attacks on blockchain systems, and more importantly, to canvass quantum-resistant cryptographic architectures

and modular blockchain design methodologies that enhance resilience. We focus on blockchain-specific impacts: digital signatures, consensus algorithms, transaction format, smart contract security, and key management. We do not attempt to cover the complete gamut of decentralized systems outside blockchains (e.g., some IoT-only DLTs or exclusively quantum network blockchains) except for comparative purposes only. The exact objectives of this paper are:

1. To survey the quantum computing algorithms (e.g., Shor's, Grover's) and threat models as they apply to blockchain layers.
2. To analyze the vulnerabilities in existing blockchain architectures, public-key infrastructure, consensus, hashing, transaction verification, smart contracts, when exposed to quantum-era adversaries.
3. To present and evaluate the major post-quantum cryptographic primitives and schemes applicable in blockchain settings, including their performance, cost, and integration trade-offs.
4. To describe architectural design patterns and migration strategies blockchains can adopt to become quantum-resistant, with minimal disruption to security, performance, and decentralization.
5. Developing a taxonomy or framework of research gaps, across theory, implementation, interoperability, standardization, and governance, requires further work before widespread quantum-resistant blockchain deployment is feasible.

By doing so, we aim to provide a technical audience (cryptographers, blockchain protocol developers, security engineers) with a brief overview of the state-of-the-art in blockchains' quantum-resistance, define areas for future research, and enable practical decisions for projects anticipating transitioning to quantum-safe systems. The rest of the paper begins with a detailed discussion of quantum algorithms and corresponding threat models (Section 2), followed by identifying blockchain vulnerabilities (Section 3). Section 4 summarizes quantum-resistant cryptographic foundations, and Section 5 overviews architecture patterns and migration techniques. Section 6 introduces our research gap taxonomy, Section 7 summarizes future research directions, and Section 8 concludes with suggestions to practitioners and researchers.

2. Quantum Threats to Blockchain Systems

2.1. Quantum Algorithms and Their Impact

Quantum computing has introduced significant threats to blockchain system security, primarily due to what Shor's and Grover's algorithms are capable of. These two algorithms use the principles of quantum mechanics to calculate what otherwise would be impossible for traditional computers to do, thereby introducing much risk to traditional cryptographic systems implemented on blockchain technology (Figure 1). Shor's algorithm, built by Peter Shor in 1994, is most notorious for how it can factor large integers efficiently, which has the immediate effect of compromising the security of most popularly used public-key cryptosystems like RSA and ECC (Elliptic Curve Cryptography) [14–16]. Shor's algorithm enables efficient factorization and discrete-logarithm computation on a sufficiently large quantum computer, breaking RSA and elliptic-curve cryptography by allowing an adversary to derive private keys from publicly exposed information [17]. Shor's algorithm's applications extend past basic decryption; its impact undermines the basis for trust that blockchain systems are founded upon. Many studies indicate that if quantum computers are developed with the ability to execute Shor's algorithm, current blockchain security solutions may be obsolete, and development will begin towards post-quantum cryptographic solutions [18,19].

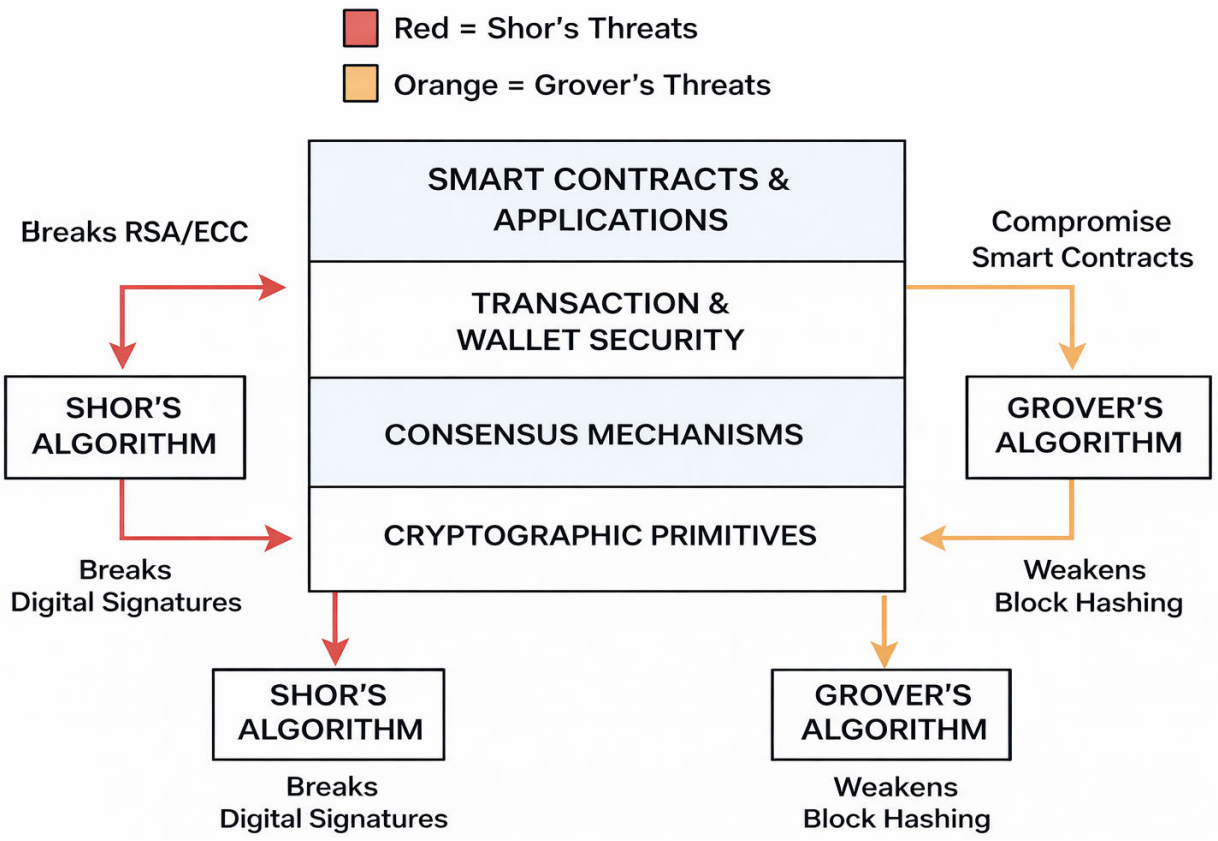

Figure 1. Attack surface diagram showing how Shor's and Grover's algorithms affect blockchain layers.

On the other hand, Grover's algorithm gives quadratic speedup to unstructured search problems, which can be very detrimental to the security of hash functions used in blockchain systems. Grover's algorithm allows a quantum computer to search for an element in a database of N items in about $\sqrt{N}$ steps, in contrast to N steps for classical algorithms [20,21]. This means that the effective security of symmetric key sizes is cut in half with quantum computing. For instance, a 256-bit key currently considered secure would provide the same level of security as a 128-bit key against a quantum attacker [18,19].

The applications of Grover's algorithm are especially noteworthy for blockchain proof-of-work mining protocols, where the efficiency of finding valid blocks can be greatly enhanced, presenting the opportunity for faster mining and greater centralization risks [18]. As blockchain systems widely use proof-of-work schemes, the ability of quantum computers to apply Grover's algorithm could disrupt the power equation in these systems, shifting the balance in favor of those with large-scale access to quantum resources.

Evidence supporting the severity of the quantum threat has been documented in recent cryptanalysis studies. Shor's algorithm has been shown to factor 2048-bit RSA and solve elliptic-curve discrete logarithms in polynomial time once sufficient quantum resources are available, directly compromising the signature schemes used in major blockchains [22–24]. Research groups have estimated that classical public-key schemes fall once quantum processors reach a scale of several thousand logical qubits, a threshold projected by multiple national laboratories and commercial quantum research units. Independent assessments of Bitcoin, Ethereum, and other leading blockchains have quantified exposure timelines by modeling attacker capabilities against signature reuse, transaction latency, and address-derivation patterns. These studies demonstrate that a quantum adversary can extract private keys from exposed public keys, forge signatures, and alter or replay transactions. Grover's algorithm further reduces the effective strength of widely deployed hash functions, presenting risks to mining difficulty calibration and block discovery. Together, these

findings constitute concrete evidence that quantum computing poses a structural threat to the cryptographic foundations that ensure blockchain integrity (Table 2) [25–27].

Table 2. Vulnerability of classical cryptographic algorithms to quantum attacks.

Algorithm	Type	Quantum Threat	Vulnerability Level
RSA-2048	Public-key	Shor's algorithm	Fully breakable
ECDSA/EdDSA	Public-key	Shor's algorithm	Fully breakable
SHA-256	Hash	Grover's algorithm	Security reduced by half
AES-256	Symmetric	Grover's algorithm	Reduced to AES-128 equivalent
Keccak-256	Hash	Grover's algorithm	Reduced preimage/second preimage resistance

2.2. Blockchain Vulnerability Landscape

The landscape of blockchain system vulnerability is intricate and encompasses multiple attack surfaces within its reach that are exploitable to malicious actors. Cryptographic mechanisms underpin traditional blockchain systems and are increasingly susceptible to quantum attacks. For instance, cryptosystems such as RSA and ECDSA, forming the foundation of digital signature schemes and message encryption, are vulnerable to being attacked by quantum algorithms such as Shor's algorithm, capable of factorizing large numbers and discrete logarithms with optimal efficiency [28]. This vulnerability requires a thorough risk analysis of blockchain components like network, mining pools, transaction verification mechanisms, and smart contracts [29].

Transaction authentication is among the most basic aspects of blockchain security. The application of public-key cryptography for verifying transactions means that quantum computers can potentially forge signatures and manipulate the records of transactions. Efforts are being made to develop post-quantum cryptographic techniques that can withstand quantum attacks. For example, integrating quantum key distribution (QKD) within blockchain frameworks has been proposed to secure the signing of transactions and give tamper-resistant key exchange [28]. Another solution would be adaptive consensus protocols in which mining difficulty is adjusted based on network load such that transaction authentication against quantum attackers can be further strengthened [30].

Consensus mechanisms are important in maintaining the integrity of decentralized networks. Traditional mechanisms like Proof of Work (PoW) and Proof of Stake (PoS) do not work in the quantum computing era, in which attackers can utilize their computational power to affect the consensus outcome. The creation of quantum-resistant consensus algorithms, such as the Quantum Byzantine Fault Tolerance (Q-BFT) mechanism, aims to address these vulnerabilities by incorporating quantum random number generation to enhance security and reduce Sybil attacks [28]. Furthermore, the General Secure Consensus Scheme (GSCS) has been proposed as a superior version of PoW with strong resistance against resource centralization and quantum attacks [31].

Smart contracts perform transactions on blockchain platforms and are the most vulnerable to quantum attacks. The immutability of smart contracts once deployed means that they cannot be updated to patch the weaknesses [32]. The DAO security breach in 2016 proved the risk of unsafe smart contracts at the expense of huge financial losses [33]. Researchers have developed frameworks like SoliAudit to mitigate such risks, which apply machine learning and fuzz testing to identify smart contract vulnerabilities [33]. Second, integrating quantum-resistant cryptographic practices into smart contracts can assist with making them more quantum-resistant (Table 3) [34].

Table 3. Blockchain components and vulnerabilities under quantum attack.

Component	Dependency	Attack Vector	Potential Impact
Digital Signatures	ECDSA/EdDSA	Shor's algorithm	Key extraction, transaction forgery
Hash Functions	SHA-256, Keccak	Grover's algorithm	Reduced preimage resistance
Consensus	Signature-based validation	Signature forgery	Block manipulation, double-spending
Wallets	Public-key exposure	Private-key recovery	Asset theft
Smart Contracts	Signature-gated operations	Forged calls or state changes	Unauthorized execution

3. Current Blockchain Architectures Under Quantum Pressure

Current blockchain architectures rely heavily on cryptographic primitives that lose their security guarantees in the post-quantum environment. Public-key mechanisms such as RSA, ECDSA, and EdDSA can be compromised by Shor's algorithm, allowing attackers to derive private keys and forge valid signatures. This risk affects transaction authentication, wallet security, and the immutability of historical records. Hash functions used in proof-of-work models also face reduced security levels under Grover's algorithm, lowering effective resistance against preimage attacks and enabling faster block discovery by adversaries with quantum resources. Consensus mechanisms that depend on signature validation, validator authentication, or committee formation become vulnerable to key extraction and signature forgery, which can disrupt block finality or enable double-spending attacks. Smart contracts are similarly exposed to the risk of signature forgery and state manipulation, as quantum adversaries can exploit weaknesses in underlying cryptographic operations that govern contract execution. These vulnerabilities demonstrate that existing blockchain architectures require systematic reinforcement to remain secure in the quantum era [35,36].

Legacy blockchain architectures, such as those for Bitcoin and Ethereum, rely on hash functions and public-key cryptography susceptible to quantum attack. As Kiktenko et al. [37] note, applying digital signatures and cryptographic hash functions on these systems is a significant risk, since quantum computers can use this vulnerability to alter blockchain information or gain an unfair advantage in mining. In addition, the increasingly complex use of Blockchain, particularly in sectors like supply chain management and Internet of Things (IoT), creates an even more demanding security scenario. For instance, Ruta et al. [38] describe how conventional trust models for supply chains are limited by the centralized control of information, something that blockchain technology aims to address via decentralized trust models. Nevertheless, the underlying cryptographic vulnerabilities are an urgent concern.

To counter the quantum attacks, developers are developing post-quantum blockchain architectures. Li et al. [39] present a lattice-based signature scheme that enhances quantum security for blockchain networks against quantum attackers. Not only does it fix the vulnerabilities of existing systems, but it is also more efficient compared to traditional cryptographic practices. A possible remedy is integrating quantum key distribution (QKD) into blockchains. Kiktenko et al. [37] outline an experimental quantum-safe blockchain platform based on applying QKD to authenticate securely, promising blockchain applications scalable and secure in a quantum world.

With the development of blockchain technology, hybrid structures are increasingly needed to combine classical and quantum-resistant elements. Wessling et al. [40] refer to the need to identify the areas in the application architecture that may leverage blockchain technology, proposing a softer approach of Blockchain interweaving with current systems. In addition, the concept of blockchain interoperability is gaining popularity, as documented by Qasse et al. [41]. Interoperability allows different blockchain networks to share informa-

tion and cooperate, supporting scalability and connectivity in response to challenges posed by quantum threats.

4. Quantum-Resistant Cryptographic Foundations

4.1. Lattice-Based Cryptography

Lattice-based cryptography is presently the leader of post-quantum cryptographic systems due to its conjectured resistance against quantum attacks. The beginning point of the foundational work was Ajtai's groundbreaking efforts, which laid the foundation for many cryptographic schemes with the hardness of lattice problems [42]. Lattice-based schemes make use of problems such as the Shortest Vector Problem (SVP) and Learning With Errors (LWE), which are believed to be hard even for a quantum computer [43]. Those efficient constructions that have been recently developed, such as the NTRU encryption scheme and the Falcon signature scheme, both of which were found in the NIST post-quantum cryptography standardization process [44], rely on lattice-based schemes.

Desirable features of lattice-based cryptography are worst-case intractability assumptions, security, parallelism, and asymptotic efficiency [43]. New structures like bonsai trees have introduced innovation in identity-based encryption and lattice-based signatures [45]. These showcase the potential of lattice-based cryptography to provide robust security in a post-quantum world.

4.2. Hash-Based Signatures

Hash signatures are another potential quantum-resistant cryptography line. Hash signature schemes utilize hash functions to produce secure digital signatures, one of the most well-known being the Merkle signature scheme. The security of hash signatures is based directly on the underlying hash function; thus, hash signatures are also resistant to quantum attacks based on weaknesses in traditional public-key schemes [46]. Studies recently have focused on enhancing the reliability of hash-based signatures by developing reliable hash trees, which have embedded error-detecting mechanisms that protect against malicious and natural faults [46,47].

4.3. Code-Based Cryptography

Code-based cryptography is mature and has existed for some time. It is also quantum-resistant. One of the most well-known code-based schemes is the McEliece encryption system based on the Syndrome Decoding Problem (SDP). It is derived from the hardness of decoding random linear codes, which remains hard for quantum computers. Current research in code-based cryptography has focused on optimizing implementations for performance and efficiency, particularly in embedded devices [48]. The standardization process at NIST has also pushed code-based schemes as front-runners for post-quantum cryptography, highlighting their potential for secure communication in a quantum world [49].

4.4. Multivariate & Isogeny-Based Approaches

Multivariate cryptography and isogeny-based cryptography are additional paradigms in the search for quantum-resistant solutions. Multivariate schemes, such as the Unbalanced Oil and Vinegar (UOV) signature scheme, are founded on the hardness of the problem of solving systems of multivariate polynomial equations, which are believed to be hard for both quantum and classical computers [50]. Isogeny-based cryptography, on the other hand, relies on the difficulty of calculating isogenies between supersingular elliptic curves. This line of research has gained popularity due to its unique mathematical properties and potential for secure key exchange protocols. However, issues with implementation efficiency and key size must be resolved to make it practical [49].

Lattice-based schemes offer the best balance of efficiency and security for Blockchain, hash-based signatures provide strong but bulky alternatives, while code-based, multivariate, and isogeny-based approaches face significant scalability or security limitations (Table 4).

Table 4. Comparative assessment of quantum-resistant cryptographic families for Blockchain.

Scheme Family	Key Size	Signature Size	Verification Speed	Blockchain Suitability
Lattice-based	Moderate (e.g., Dilithium 897–1760 bytes)	Moderate (e.g., Dilithium signatures ~1–2 KB)	High (Dilithium fastest, verification very efficient)	Highly suitable: Efficient, mature, selected by NIST standards, good security/performance balance
Hash-based	Small to Moderate	Large (SPHINCS+ has large signatures)	Moderate to Slow	Suitable: Strong security from hash functions, signature size trade-off limits throughput
Code-based	Large (McEliece public keys are very large, sometimes >10 KB)	Moderate to Large	Moderate to Slow	Limited suitability: Large key sizes pose storage/transfer challenges
Multivariate-based	Moderate to Large	Moderate to Large	Moderate	Experimental/limited: Some schemes broken, but potential for quantum resistance
Isogeny-based	Small	Small	Slow (recent attacks have undermined security)	Limited suitability: Key size compactness is good, but recent cryptanalysis has made them less secure

5. Architectural Approaches for Quantum-Resilient Blockchains

The advent of quantum computing necessitates a blockchain architectural re-engineering that transcends the simple substitution of cryptography. Since quantum adversaries can theoretically compromise elliptic curve digital signatures (ECDSA, EdDSA) and undermine the security assumptions of proof-of-work or proof-of-stake chains, researchers have explored holistic approaches to making blockchains quantum-resistant.

One of the earliest architectural considerations is the use of modular security layers. Most legacy blockchains have cryptographic primitives tightly coupled with consensus, transaction validation, and network layers. For instance, Bitcoin integrates ECDSA directly into transaction formats, and Ethereum has elliptic-curve operations as part of the virtual machine opcodes. The tight integration ensures that cryptographic agility is difficult, as upgrading means changing consensus-critical components. A modular security model, by contrast, separates cryptography from higher-level blockchain functionalities. In this design, consensus, transaction validation, and key management are decoupled into their own layers, each free to evolve independently. This modularity mirrors the separation of concerns in traditional network security systems, where TLS and IPsec are beneath application protocols. Modular architectures such as these facilitate the transition to post-quantum cryptography (PQC) and future-proof systems against unforeseen cryptanalytic breakthroughs, enabling blockchains to switch algorithms as standards evolve [35,36].

The second approach is the deployment of hybrid cryptographic primitives, where classical and post-quantum algorithms are executed in parallel. Because of uncertainty about the long-term effectiveness and security of PQC candidates, a transition mechanism is necessary to ensure both backward compatibility and forward security. Hybrid cryptography, a concept already adopted by groups like the Internet Engineering Task Force (IETF) and NIST for TLS, is also relevant to blockchain signatures and key exchanges. For

example, a transaction might require two signatures in parallel: one with ECDSA (classical) and the other with CRYSTALS-Dilithium (post-quantum). Verification succeeds only if both are valid, offering security against classical and quantum attackers [51]. Similarly, hybrid key encapsulation mechanisms can combine elliptic-curve Diffie–Hellman with lattice-based KEMs such as Kyber. While this approach incurs signature size and verification costs, it does provide a safety net during the uncertain standardization of PQC. Regarding blockchain deployment, hybrid schemes can be deployed incrementally, on a phase-by-phase basis, where dual validation during a transition period would be mandated by smart contracts or wallet software before the retirement of classical primitives. Hybridization, therefore, trades off risk reduction against operational continuity, but must be designed carefully to avoid inflating transaction sizes and network traffic [52].

A third architectural approach entails migration frameworks to move incumbent blockchains to quantum-safe primitives. Migration is perhaps the most difficult issue, as blockchains are immutable and decentralized by construction. As opposed to traditional systems in which cryptographic updates can be centrally enforced, blockchain networks require community consensus to implement protocol updates. Several migration paths have been proposed. One possibility is a hard fork, in which the Blockchain splits into two versions: one that adopts PQC and one that retains the legacy schemes. This provides a clean break but risks fragmentation and loss of trust, as seen in previous forks like Ethereum/Ethereum Classic. Soft forks make the subtler solution, adding new rules while remaining backward compatible with current blocks. New addresses, for instance, would be spent with PQC signatures, but legacy addresses would still be spendable and only phased out over time. However, soft forks have limits in enacting universal adoption without sacrificing decentralization. Another strategy is backward-compatible transaction formats, where addresses support multiple signature verification scripts, allowing wallets to migrate incrementally. For example, Bitcoin's Segregated Witness (SegWit) introduced flexible scripting that can, in theory, support PQC alongside ECDSA. Migration also requires key rotation methods, enabling users to move funds from classical keys to PQC keys without exposure to "store now, decrypt later" attacks, where attackers intercept classical signatures today for quantum use later. Migration to Blockchain is thus not a solely technical process but a socio-technical process involving governance, incentives, and user education [26].

Re-engineering of consensus is a fourth architectural direction. Quantum attacks do not directly threaten traditional proof-of-work (PoW) consensus protocols since the quadratic speedup provided by Grover's algorithm is for hash preimages and not exponential. However, proof-of-stake (PoS) and Byzantine fault-tolerant (BFT) consensus protocols heavily depend on digital signatures for block validation, committee formation, and message authentication. For example, Ethereum 2.0's PoS requires validators to sign attestations and blocks; if quantum adversaries break ECDSA, attackers can forge validator votes, undermining finality. Re-designing consensus protocols with PQC is therefore necessary. One answer is replacing signature schemes with lattice-based ones that provide fast verification and batch aggregation, allowing scalability. Dilithium or Falcon signatures, for instance, can be integrated into BFT-style consensus systems, where message complexity is already high. Another path is the study of quantum-secure randomness beacons for validator selection, which would avoid manipulation risks in stake-based systems. Consensus redesign can also consider PQC-friendly threshold signature schemes, where validator groups jointly produce signatures based on post-quantum primitives. The challenge lies in minimizing the performance overheads, since BFT systems are already susceptible to communication bottlenecks that can be compounded with more computationally intensive cryptographic operations [53,54].

Finally, scalability and performance trade-offs must be dealt with holistically. Post-quantum proposals usually have larger key sizes, signature sizes, and computational overheads than classical elliptic-curve cryptography. For example, a Dilithium-III signature is approximately 2.7 KB, while an ECDSA signature is 64 bytes, and SPHINCS+ signatures can be 16–30 KB. These overheads significantly affect block size, propagation latency, and storage requirements for high-throughput blockchains with thousands of transactions per second. Also, consensus protocols relying on frequent signature verifications may see throughput reductions if PQC operations are computationally intensive.

Trade-offs among the security level, efficiency, and decentralization goals exist. Low-weight PQC schemes, such as Falcon with small signatures (~666 bytes), offer promising bandwidth cost savings but impose tight constraints for floating-point arithmetic that make implementations difficult. Similarly, code-based proposals like McEliece enjoy fast decryption but enormous public keys, which are poorly suited to lightweight wallet hardware or blockchains with high address churn. Scalability concerns extend from transaction signing to the execution of smart contracts, where PQC can bloat gas fees and deter complex operations. Batching and aggregation techniques, like lattice-based aggregate signatures or Merkle tree compression, have been proposed by researchers to counteract scalability. However, these optimizations introduce further complexity in verification logic and can affect interoperability with existing smart contract languages. Balancing quantum resilience with performance remains an open research question with careful parameter tuning and benchmarking across blockchain environments [55]. Table 5 compares various post-quantum cryptography approaches based on their security, scalability, performance, governance and adoption challenges, and integration complexity.

Table 5. Comparison of post-quantum cryptography approaches.

Approach	Security	Scalability/Performance	Governance/Adoption	Integration Complexity
Modular Security Layers	High: Easy upgrades & algorithm swaps	Medium: Slight overhead	Medium: Requires standardization	Medium: Needs architectural refactoring
Hybrid Cryptography	Very High: Dual protection	Low–Medium: Larger signatures	High: Incremental adoption	Medium: Dual verification logic
Migration Strategies	High: Maintains security across upgrades	Medium: Possible throughput/storage impact	Medium–High: Community coordination required	High: Protocol & wallet updates needed
Consensus Re-Engineering	High: PQC in validator signatures	Medium: Larger messages, verification cost	Medium: Validator adoption needed	High: Consensus modifications
Scalability/Performance Trade-offs	Medium–High: Balances security & efficiency	Low–Medium: Larger keys/signatures	Medium: User acceptance required	Medium: Optimization techniques needed

6. Taxonomy of Research Gaps and Challenges

6.1. Theoretical Gaps

Traditional security models used to analyze cryptographic protocols, such as the random oracle model (ROM), might not be able to realize the security picture when quantum attackers are considered. In the classical ROM, hash functions are modeled as perfectly random oracles, but in a quantum world, the oracles may be superposition queried by quantum attackers, and therefore, information might be leaked that would be hidden in the classical scenario. This entails using the quantum random oracle model (QROM) for more secure proofs [56].

Quantum random oracle proofs are far more challenging than traditional ROM proofs. Fukumitsu and Hasegawa [56] note the complexity of programming the random oracle in the security proof within the QROM. They counteract this by proposing novel proof techniques, combining existing methods with new programming techniques. Their work provides a lattice-based multisignature scheme whose security is proven in the QROM, advancing post-quantum cryptography on blockchains. Yang et al. [57] note that much work has been carried out on examining subversion attacks (delicate manipulation of cryptographic implementation to leak information), but work on the subject within the context of post-quantum cryptography is not much. They exhibit a subversion attack against an encryption scheme constructed from lattices, demonstrating the need for more robust security models accounting for such attacks in the post-quantum world.

6.2. Technical Gaps

Many PQC schemes require significantly more computational resources than their classical counterparts. This extra use of resources can lead to decreased processing speeds for transactions and higher operating costs, which are critical factors for blockchain networks that are concerned about speed and cost-effectiveness. For instance, PQC can demand larger key sizes and more complex mathematical calculations, which can overwhelm the limited computation capacity of specific blockchain nodes [58].

In addition to efficiency, the design of key cryptography and blockchain system architecture sizes can also be a limitation. The higher key sizes of PQC can be a source of increased space and bandwidth consumption, which may not be feasible with all blockchain applications. Most present-day blockchain systems are not designed to accommodate the peculiar requirements of PQC, leading to incompatibility that can make the integration process challenging [59].

More sophisticated architectural designs for blockchain systems aim to enhance scalability, security, and interoperability. Such proposals typically have their trade-offs that ultimately limit their practical application. In some architectures, for example, enhancing transaction throughput can mean adding increasing complexities that make them less user-friendly or more difficult to deploy [60].

One of the normal trade-offs in blockchain architecture is security vs. scalability. Most likely solutions, such as sharding or layer-2 protocols, aim to increase transaction capacity at the possible expense of security guarantees that support blockchain technology. This trade-off can deter organizations from adopting these solutions since they may put security first and sacrifice performance [61].

Interoperability between multiple blockchain systems is another significant issue. As multiple blockchain networks emerge, the ability to talk and conduct business over these networks is of utmost significance. However, significant alterations to existing architectures must be implemented to achieve interoperability, which will be expensive and formidable. This can discourage organizations from adopting new systems, particularly if they are already invested in existing technologies [62].

Technical gaps remain in integrating PQC into blockchain environments, including substantial increases in key and signature sizes, higher computational overhead for transaction validation, and limited support within current block formats and virtual machines. These constraints affect network throughput, block propagation, and node resource requirements. Several studies emphasize the need for optimized PQC implementations, hardware acceleration, and protocol-level redesign to support post-quantum primitives on scalable decentralized systems.

6.3. Implementation Gaps

Implementation gaps can be due to many reasons, including technological limitations, regulatory complexities, and the indigenous nature of blockchain complexity. For instance, blockchain technology, as decentralized and secure, actually reveals loopholes and inefficiencies that are not apparent during prototyping [63]. Migration strategies must be in place to shift from one blockchain protocol to another or upgrade existing systems without significant disruptions. The concept of "live gang migration," studied by Deshpande et al., highlights the importance of optimizing the migration of multiple colocated virtual machines (VMs) for minimizing downtime and resource usage [64].

The challenges of upgrading the blockchain system include data integrity, consensus maintenance, and network traffic management. Zhao et al. highlight the requirement for innovative solutions to facilitate simple upgradeability in blockchain applications, particularly in finance and supply chain management [65]. Several studies have investigated actual deployments of blockchain technologies that highlight the necessity of bridging implementation gaps. For instance, Pustisek et al. [66] explain the implementation of Blockchain in self-driving electric charging station choice, where they point out the role of smart contracts in facilitating real-time decision-making within a decentralized system.

Similarly, Chen and Zhu [67] provide a blockchain personal archive service system emphasizing secure and effective data handling in decentralized systems. The problems faced in such applications tend to mirror those found in broader blockchain systems, further justifying the necessity of proper migration and upgradeability planning.

6.4. Adoption & Governance Gaps

The social context in which blockchain technologies are introduced is important to their adoption. Their perception and cognitive frames heavily drive the users' adoption of new technologies. Lin and Silva [68] state that adopting information systems is a political and social process. The stakeholders frame and reframe their perceptions based on their experience and the context in which they evaluate the technology. This dynamic nature of cognitive frames suggests that for quantum-resistant blockchain systems to be adopted, stakeholders must be engaged in a way that addresses their concerns and perceptions about the technology.

Social structure and technology adoption have been extensively documented to be related. Damanpour et al. [69] firmly established that changes in social structure, such as utilizing administrative innovations, can result in subsequent technical system changes. This, in turn, implies that there must be a conducive environment to facilitate the successful implementation of quantum-resistant blockchain technologies.

Organizational readiness and support are among the foremost determinants of technology adoption. Research conducted by Clohessy and Acton [70] points out that top management support and organizational readiness are the enablers of adopting Blockchain. For quantum-resistant systems, organizations must be technically, structurally, and culturally prepared to implement innovations of this kind. The findings of Kamble et al. [71] also indicate that ease of use and perceived usefulness are key drivers for blockchain adoption, and these can be extended to quantum-resistant technology.

According to Lee et al. [67], organizational innovation commitment is central. Organizations that considerably invest in research and development in advanced technologies have a greater chance of adopting quantum-resistant technologies. This commitment can be achieved through training and sensitization programs that equip employees with the necessary capacity and knowledge to comprehend and apply such technologies effectively. Jurisdictions differ in regulating Blockchain, which can cause confusion and detract from the adoption cause. For quantum-resistant blockchain systems, regulatory clarity is nec-

essary to provide confidence and guidance to organizations considering their adoption. Inadequate legal and regulatory support has been identified as the major inhibitor of Blockchain within e-government contexts [72]. Figure 2 shows a taxonomy diagram for blockchain security in the quantum era.

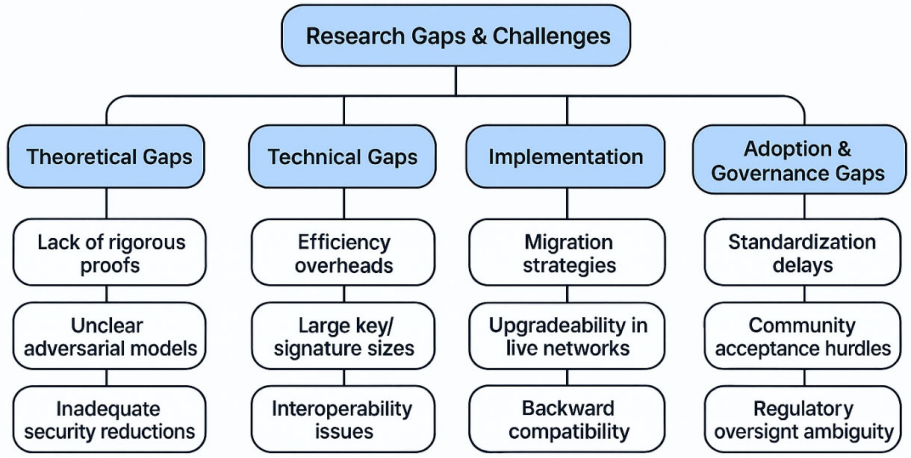

Figure 2. Taxonomy diagram mapping gaps into four categories with subnodes.

7. Future Directions and Open Questions

With quantum computing evolving at a high speed, there is a pressing need for the blockchain community to prepare for and mitigate potential threats. Although post-quantum cryptography (PQC) has developed a lot, there are still various open issues concerning its practical implementation in decentralized networks. One of the main future directions is the standardization of quantum-resistant primitives. The ongoing NIST PQC process has already selected some candidate algorithms for standardization, including lattice-based key encapsulation mechanisms (Kyber), digital signatures (Dilithium, Falcon), and stateless hash-based signatures (SPHINCS+). While these selections provide a foundation for quantum-resistant blockchains, the implications on deployed systems are not straightforward. Rolling out these algorithms to live blockchain networks requires careful handling of transaction formats, block size limits, signature verification throughput, and backward compatibility. Standards development may also necessitate continuous updating of blockchain nodes, wallet software, and smart contracts. Therefore, there is a motivation for developing agile, modular blockchain architectures that can readily accommodate new post-quantum algorithms as standardization evolves.

Another promising direction is the exploration of new consensus mechanisms for the post-quantum world. While classical proof-of-work (PoW) and proof-of-stake (PoS) protocols rely heavily on elliptic-curve cryptography and hash-based proofs, quantum adversaries can undermine signature schemes used in block validation and validator selection. It is important to develop consensus protocols that either minimize the reliance on compromised primitives or inherently encompass post-quantum cryptography. Potential solutions include threshold signatures with PQC, lattice-based VRFs for validator selection, or hybrid consensus protocols that combine some quantum-resilient primitives. Additional research is necessary to quantify trade-offs in security, throughput, and decentralization for such reengineered protocols to ensure that quantum-resistant consensus protocols remain feasible for large-scale deployments.

Interdisciplinary approaches will also be critical to the achievement of quantum-resistant blockchains. Hardware acceleration is one direction, leveraging special-purpose processors such as FPGAs or GPUs to speed up the computationally intensive operations of lattice-based or code-based schemes. Quantum-safe network protocols, including se-

cure key exchange and encrypted communication channels between nodes, are another vital layer of defense. Combining cryptography, hardware, and network-level protection will require collaboration among computer science, electrical engineering, and applied mathematics collaboration. In this way, interdisciplinary research can achieve performance improvement, low latency, and energy efficiency, which are particularly important for high-throughput blockchains and IoT-integrated decentralized networks.

Finally, the long-term vision for blockchain research is the realization of blockchain networks that are simultaneously quantum-secure, scalable, and energy-efficient. Bringing this vision to fruition entails addressing several open questions. Can post-quantum signature schemes be streamlined for compact transaction size and verification costs without compromising security? How can blockchain protocols maintain high throughput and low latency while supporting larger keys and signatures inherent in PQC? What are the best incremental adoption and governance strategies for decentralized networks with heterogeneous participants? Energy consumption remains a primary concern: quantum-resistant schemes need to at least equal or improve the energy efficiency of existing protocols, especially as the environmental footprint is increasingly a concern.

8. Conclusions

The rapid emergence of quantum computing poses a profound challenge to the security underpinnings of blockchain technology. Old cryptographic primitives, such as elliptic-curve signatures and RSA key exchanges, supply decentralized systems' integrity, authenticity, and unchangeability. But quantum algorithms, above all, Shor's algorithm, are likely to be able to crack the underlying mathematical hurdles of these primitives, opening up present blockchains to forgery, double-spending, and network compromise. In principle, even modestly sized quantum computers would enable attackers to retroactively manipulate stored blockchain information retroactively, highlighting the need for pre-emptive quantum-resistant practices. The scale of the quantum risk is amplified by the decentralized and unalterable nature of blockchains: global edits post-deployment require coordinated migration and public consensus, which are by their very nature gradual processes. Therefore, it is imperative to know the extent of the threat and prepare for robust architectures to protect blockchain environments before the advent of massive-scale quantum computers.

To meet this looming danger, numerous quantum-resistant cryptographic protocols have emerged. Lattice-based ones, such as CRYSTALS-Kyber and Dilithium, have proven to provide decent performance-security trade-offs for key exchange and digital signatures. Hash-based signatures, such as XMSS and SPHINCS+, provide provable security under reasonable assumptions solely on the preimage security of hash functions, but with higher signatures and computational overhead. Code-oriented approaches like Classic McEliece provide fast encapsulation and excellent long-term security at the expense of extremely large public keys. Multivariate and isogeny-based cryptography, while theoretically fascinating and compact in certain applications, possesses open cryptanalytic problems or is too complicated to realize. At the same time, architectural compromises like modular security layers, hybrid cryptography, migration frameworks, and consensus re-engineering provide windows into deploying these post-quantum building blocks into live blockchain networks without undermining decentralization or operational continuity. The combined strength of cryptographic innovation and architectural flexibility is the most promising route for rendering blockchain networks immune to existing and future quantum assaults.

One of the insights of this review is that the problem of post-quantum blockchain security is wider than choosing a single cryptographic algorithm. Mitigation must be holistic, balancing performance, scalability, governance, and energy efficiency. Modular architectures enable blockchains to implement new algorithms piecemeal and minimize

disruption when migrating. Hybrid architectures provide double security during times of transition, whereas migration schemes, hard forks, soft upgrades, or backward-compatible variants, address the challenges of decentralized decision-making. Consensus algorithms must be rearchitected to accommodate quantum-resistant signatures and threshold schemes with guaranteed validator selection and block finality. Scalability parameters like signature size, verification latency, and block propagation must be approached cautiously, not to degrade throughput or user experience. These strategies illustrate that a successful post-quantum transition necessitates harmonization among cryptographic research, system architecture, and community governance.

In the future, the ratio of innovation to safe migration is crucial. While quantum-resistant primitives need to be rapidly adopted on one hand to pre-empt adversaries and provide trust in blockchain networks, uncoordinated or premature migration risks fragmentation of the network, bad performance, or unintended vulnerabilities on the other hand. Standardization efforts, particularly the NIST PQC process, are the critical foundation for informed decision-making, enabling blockchain developers to select tried algorithms with well-established security and performance characteristics. Research will continue to mature cryptographic primitives and system designs, including hardware acceleration, quantum-resistant networking, and scalable consensus algorithms. They aim to create secure, efficient, and adaptable blockchains that are resilient against quantum attacks and evolving technological and regulatory landscapes.

Quantum computing is both a threat and a potential for blockchain networks. The threat points to the weakness of classical cryptographic assumptions, while the opportunity lies in redesigning blockchain architecture with innovative, quantum-resistant designs. With the integration of lattice, hash-based, and code-based cryptography into modular, hybrid, and performance-optimized architectures, the blockchain ecosystem can chart a path to safe, scalable, and sustainable networks. The ultimate objective is to ensure that Blockchain is still a dependable, decentralized book of records in the era of powerful quantum adversaries, finding a balance between innovation and robust and secure migration strategies.

Funding: This research received no external funding.

Data Availability Statement: No data was used for this research.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Du, M.; Ma, X.; Zhang, Z.; Wang, X.; Chen, Q. A review on consensus algorithm of blockchain. In *Proceedings of the 2017 IEEE International Conference On Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, 5–8 October 2017*; IEEE: Piscataway, NJ, USA, 2017; pp. 2567–2572.
2. Stephen, R.; Alex, A. A review on blockchain security. *IOP Conf. Ser. Mater. Sci. Eng.* **2018**, *396*, 012030. [CrossRef]
3. Taherdoost, H.; Mohamed, N.; Farhaoui, Y.; Prasad, M.; Pham, T.T.L.; Le, T.-V. Blockchain Models Applications: A Comparative Study on Security. *Procedia Comput. Sci.* **2025**, *258*, 1003–1011. [CrossRef]
4. Helo, P.; Hao, Y. Blockchains in operations and supply chains: A model and reference implementation. *Comput. Ind. Eng.* **2019**, *136*, 242–251. [CrossRef]
5. Fraga-Lamas, P.; Fernández-Caramés, T.M. A review on blockchain technologies for an advanced and cyber-resilient automotive industry. *IEEE Access* **2019**, *7*, 17578–17598. [CrossRef]
6. Tariq, N.; Asim, M.; Al-Obeidat, F.; Zubair Farooqi, M.; Baker, T.; Hammoudeh, M.; Ghafir, I. The security of big data in fog-enabled IoT applications including blockchain: A survey. *Sensors* **2019**, *19*, 1788. [CrossRef] [PubMed]
7. Kearney, J.J.; Perez-Delgado, C.A. Vulnerability of blockchain technologies to quantum attacks. *Array* **2021**, *10*, 100065. [CrossRef]
8. Khodaiemehr, H.; Bagheri, K.; Feng, C. Navigating the quantum computing threat landscape for blockchains: A comprehensive survey. *Authorea* **2023**. [CrossRef]

9. Ullah, M.; Ali, A.; Jadoon, A.K. Quantum Computing and Blockchain Security: A Critical Assessment of Cryptographic Vulnerabilities and Post-Quantum Migration Strategies. *Policy Res. J.* **2025**, *3*, 159–172.
10. Fernandez-Carames, T.M.; Fraga-Lamas, P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access* **2020**, *8*, 21091–21116. [CrossRef]
11. Gai, K.; Guo, J.; Zhu, L.; Yu, S. Blockchain meets cloud computing: A survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2009–2030. [CrossRef]
12. Hemdan, E.E.-D.; El-Shafai, W.; Sayed, A. Integrating digital twins with IoT-based blockchain: Concept, architecture, challenges, and future scope. *Wirel. Pers. Commun.* **2023**, *131*, 2193–2216. [CrossRef] [PubMed]
13. Yang, Z.; Alfauri, H.; Farkiani, B.; Jain, R.; Di Pietro, R.; Erbad, A. A survey and comparison of post-quantum and quantum blockchains. *IEEE Commun. Surv. Tutor.* **2023**, *26*, 967–1002. [CrossRef]
14. Petrenko, A. *Applied Quantum Cryptanalysis*; River Publishers: Aalborg, Denmark, 2023.
15. Assa-Agyei, K. Enhancing the Performance of Cryptographic Algorithms for Secured Data Transmission. Ph.D. Thesis, Nottingham Trent University, Nottingham, UK, 2024.
16. Olaoye, G. Quantum Cryptanalysis: Breaking Classical Encryption with Shor's and Grover's Algorithms. *Authorea* **2025**. [CrossRef]
17. Shen, R.; Xiang, H.; Zhang, X.; Cai, B.; Xiang, T. Application and implementation of multivariate public key cryptosystem in blockchain (short paper). In *Proceedings of the International Conference on Collaborative Computing: Networking, Applications and Worksharing, London, UK, 19–22 August 2019*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 419–428.
18. Allende, M.; León, D.L.; Cerón, S.; Pareja, A.; Pacheco, E.; Leal, A.; Da Silva, M.; Pardo, A.; Jones, D.; Worrall, D.J. Quantum-resistance in blockchain networks. *Sci. Rep.* **2023**, *13*, 5664. [CrossRef] [PubMed]
19. Chauhan, S.; Ojha, V.P.; Yarahmadian, S.; Carvalho, D. Towards building quantum resistant blockchain. In *Proceedings of the 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 16–17 November 2023*; IEEE: Piscataway, NJ, USA, 2023; pp. 1–9.
20. Brassard, G.; Høyer, P.; Tapp, A. Quantum counting. In *Proceedings of the International Colloquium on Automata, Languages, and Programming, Aalborg, Denmark, 13–17 July 1998*; Springer: Berlin/Heidelberg, Germany, 1998; pp. 820–831.
21. Giri, P.R.; Korepin, V.E. A review on quantum search algorithms. *Quantum Inf. Process.* **2017**, *16*, 315. [CrossRef]
22. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994*; IEEE: Piscataway, NJ, USA, 1994; pp. 124–134.
23. Gidney, C.; Ekerå, M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum* **2021**, *5*, 433. [CrossRef]
24. Chevignard, C.; Fouque, P.-A.; Schrottenloher, A. Reducing the number of qubits in quantum factoring. In *Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 2025*; Springer: Berlin/Heidelberg, Germany, 2025; pp. 384–415.
25. Chen, L.; Chen, L.; Jordan, S.; Liu, Y.-K.; Moody, D.; Peralta, R.; Perlner, R.A.; Smith-Tone, D. *Report on Post-Quantum Cryptography*; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2016; Volume 12.
26. Aggarwal, D.; Brennen, G.K.; Lee, T.; Santha, M.; Tomamichel, M. Quantum attacks on Bitcoin, and how to protect against them. *arXiv* **2017**, arXiv:1710.10377. [CrossRef]
27. Roetteler, M.; Naehrig, M.; Svore, K.M.; Lauter, K. Quantum resource estimates for computing elliptic curve discrete logarithms. In *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Hong Kong, China, 3–7 December 2017*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 241–270.
28. Reddy, N.R.; Suryadevara, S.; Reddy, K.G.R.; Umamaheswari, R.; Guttula, R.; Kotoju, R. Quantum secured blockchain framework for enhancing post quantum data security. *Sci. Rep.* **2025**, *15*, 31048. [CrossRef]
29. Baseri, Y.; Hafid, A.; Shahsavari, Y.; Makrakis, D.; Khodaiemehr, H. Blockchain Security Risk Assessment in Quantum Era, Migration Strategies and Proactive Defense. *arXiv* **2025**, arXiv:2501.11798. [CrossRef]
30. Alsadi, N.; Giuliano, A.; Gadsden, S.A.; Yawney, J. An adaptive approach to blockchain in smart system applications. In *Proceedings of the Big Data V: Learning, Analytics, and Applications, Orlando, FL, USA, 1–2 May 2023*; SPIE: Bellingham, WA, USA, 2023; pp. 27–32.
31. Wang, J.; Ding, Y.; Xiong, N.N.; Yeh, W.-C.; Wang, J. GSCS: General secure consensus scheme for decentralized blockchain systems. *IEEE Access* **2020**, *8*, 125826–125848. [CrossRef]
32. Taherdoost, H. Smart contracts in blockchain technology: A critical review. *Information* **2023**, *14*, 117. [CrossRef]
33. Liao, J.-W.; Tsai, T.-T.; He, C.-K.; Tien, C.-W. Soliaudit: Smart contract vulnerability assessment based on machine learning and fuzz testing. In *Proceedings of the 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, 22–25 October 2019*; IEEE: Piscataway, NJ, USA, 2019; pp. 458–465.
34. Chen, J.; Gan, W.; Hu, M.; Chen, C.-M. On the construction of a post-quantum blockchain for smart city. *J. Inf. Secur. Appl.* **2021**, *58*, 102780. [CrossRef]

35. Mosca, M. Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Secur. Priv.* **2018**, *16*, 38–41. [CrossRef]
36. Wang, Y.; Ismail, E.S. A Review on the Advances, Applications, and Future Prospects of Post-Quantum Cryptography in Blockchain, IoT. *IEEE Access* **2025**, *13*, 112962–112977. [CrossRef]
37. Kiktenko, E.O.; Pozhar, N.O.; Anufriev, M.N.; Trushechkin, A.S.; Yunusov, R.R.; Kurochkin, Y.V.; Lvovsky, A.; Fedorov, A.K. Quantum-secured blockchain. *Quantum Sci. Technol.* **2018**, *3*, 035004. [CrossRef]
38. Ruta, M.; Scioscia, F.; Ieva, S.; Capurso, G.; Di Sciascio, E. Supply chain object discovery with semantic-enhanced blockchain. In Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems, Delft, The Netherlands, 6–8 November 2017; pp. 1–2.
39. Li, C.-Y.; Chen, X.-B.; Chen, Y.-L.; Hou, Y.-Y.; Li, J. A new lattice-based signature scheme in post-quantum blockchain network. *IEEE Access* **2018**, *7*, 2026–2033. [CrossRef]
40. Wessling, F.; Ehmke, C.; Hesenius, M.; Gruhn, V. How much blockchain do you need? towards a concept for building hybrid dapp architectures. In Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, Gothenburg, Sweden, 27 May 2018; pp. 44–47.
41. Qasse, I.A.; Abu Talib, M.; Nasir, Q. Inter blockchain communication: A survey. In Proceedings of the ArabWIC 6th Annual International Conference Research Track, Rabat, Morocco, 7–9 March 2019; pp. 1–6.
42. Regev, O. Lattice-based cryptography. In *Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2006*; Springer: Berlin/Heidelberg, Germany, 2006; pp. 131–141.
43. Peikert, C. A decade of lattice cryptography. *Found. Trends Theor. Comput. Sci.* **2016**, *10*, 283–424. [CrossRef]
44. Richter, M.; Bertram, M.; Seidensticker, J.; Tschache, A. A mathematical perspective on post-quantum cryptography. *Mathematics* **2022**, *10*, 2579. [CrossRef]
45. Cash, D.; Hofheinz, D.; Kiltz, E.; Peikert, C. Bonsai trees, or how to delegate a lattice basis. *J. Cryptol.* **2012**, *25*, 601–639. [CrossRef]
46. Mozaffari-Kermani, M.; Azarderakhsh, R. Reliable hash trees for post-quantum stateless cryptographic hash-based signatures. In *Proceedings of the 2015 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS), Amherst, MA, USA, 12–14 October 2015*; IEEE: Piscataway, NJ, USA, 2015; pp. 103–108.
47. Mozaffari-Kermani, M.; Azarderakhsh, R.; Aghaie, A. Fault detection architectures for post-quantum cryptographic stateless hash-based secure signatures benchmarked on ASIC. *ACM Trans. Embed. Comput. Syst. (TECS)* **2016**, *16*, 1–19. [CrossRef]
48. Alnaseri, O.; Himeur, Y.; Atalla, S.; Mansoor, W. Complexity of Post-Quantum Cryptography in Embedded Systems and Its Optimization Strategies. In *Proceedings of the 2025 International Wireless Communications and Mobile Computing (IWCMC), Abu Dhabi, United Arab Emirates, 12–16 May 2025*; IEEE: Piscataway, NJ, USA, 2025; pp. 776–781.
49. Cherkaoui Dekkaki, K.; Tasic, I.; Cano, M.-D. Exploring post-quantum cryptography: Review and directions for the transition process. *Technologies* **2024**, *12*, 241. [CrossRef]
50. Bai, Y.; Kim, A.; Seo, S.-H. A Comparison of NIST 2nd Round Candidates' MQ-based Signature Schemes. In *Proceedings of the 2019 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 16–18 October 2019*; IEEE: Piscataway, NJ, USA, 2019; pp. 41–46.
51. Bindel, N.; Brendel, J.; Fischlin, M.; Goncalves, B.; Stebila, D. Hybrid key encapsulation mechanisms and authenticated key exchange. In *Proceedings of the International Conference on Post-Quantum Cryptography, Chongqing, China, 8–10 May 2019*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 206–226.
52. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
53. Boneh, D.; Drijvers, M.; Neven, G. Compact multi-signatures for smaller blockchains. In *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, Australia, 2–6 December 2018*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 435–464.
54. Esgin, M.F.; Steinfeld, R.; Liu, J.K.; Liu, D. Lattice-based zero-knowledge proofs: New techniques for shorter and faster constructions and applications. In *Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2019*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 115–146.
55. Albrecht, M.R.; Player, R.; Scott, S. On the concrete hardness of learning with errors. *J. Math. Cryptol.* **2015**, *9*, 169–203. [CrossRef]
56. Fukumitsu, M.; Hasegawa, S. A lattice-based provably secure multisignature scheme in quantum random oracle model. In *Proceedings of the International Conference on Provable Security, Singapore, 29 November–1 December 2020*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 45–64.
57. Yang, Z.; Chen, R.; Li, C.; Qu, L.; Yang, G. On the security of LWE cryptosystem against subversion attacks. *Comput. J.* **2020**, *63*, 495–507. [CrossRef]
58. Lipasti, M.H.; Schmidt, W.J.; Kunkel, S.R.; Roediger, R.R. SPAID: Software prefetching in pointer-and call-intensive environments. In *Proceedings of the 28th Annual International Symposium on Microarchitecture, Ann Arbor, MI, USA, 29 November–1 December 1995*; IEEE: Piscataway, NJ, USA, 1995; pp. 231–236.

59. Eurlings, M.; van Setten, E.; Torres, J.A.; Dusa, M.V.; Socha, R.J.; Capodieci, L.; Finders, J. 0.11-um imaging in KrF lithography using dipole illumination. In *Proceedings of the Lithography for Semiconductor Manufacturing II, Edinburgh, UK, 30 May–1 June 2001*; SPIE: Cergy-Pontoise, France, 2001; pp. 266–278.
60. Poteete, A.R.; Ostrom, E. Fifteen years of empirical research on collective action in natural resource management: Struggling to build large-N databases based on qualitative research. *World Dev.* **2008**, *36*, 176–195. [CrossRef]
61. Peng, R.; Xiong, L.; Yang, Z. Exploring tourist adoption of tourism mobile payment: An empirical analysis. *J. Theor. Appl. Electron. Commer. Res.* **2012**, *7*, 21–33. [CrossRef]
62. Moores, T.T. Towards an integrated model of IT acceptance in healthcare. *Decis. Support Syst.* **2012**, *53*, 507–516. [CrossRef]
63. Gao, W.; Hatcher, W.G.; Yu, W. A survey of blockchain: Techniques, applications, and challenges. In *Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 30 July–2August 2018*; IEEE: Piscataway, NJ, USA, 2018; pp. 1–11.
64. Deshpande, U.; Wang, X.; Gopalan, K. Live gang migration of virtual machines. In Proceedings of the 20th International Symposium on High Performance Distributed Computing, San Jose, CA, USA, 8–11 June 2011; pp. 135–146.
65. Zhao, J.L.; Fan, S.; Yan, J. Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financ. Innov.* **2016**, *2*, 28. [CrossRef]
66. Pustišek, M.; Kos, A.; Sedlar, U. Blockchain based autonomous selection of electric vehicle charging station. In *Proceedings of the 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI), Beijing, China, 20–21 October 2016*; IEEE: Piscataway, NJ, USA, 2016; pp. 217–222.
67. Chen, Z.; Zhu, Y. Personal archive service system using blockchain technology: Case study, promising and challenging. In *Proceedings of the 2017 IEEE International Conference on AI & Mobile Services (AIMS), Honolulu, HI, USA, 25–30 June 2017*; IEEE: Piscataway, NJ, USA, 2017; pp. 93–99.
68. Lin, A.; Silva, L. The social and political construction of technological frames. *Eur. J. Inf. Syst.* **2005**, *14*, 49–59. [CrossRef]
69. Damanpour, F.; Szabat, K.A.; Evan, W.M. The relationship between types of innovation and organizational performance. *J. Manag. Stud.* **1989**, *26*, 587–602. [CrossRef]
70. Clohessy, T.; Acton, T. Investigating the influence of organizational factors on blockchain adoption: An innovation theory perspective. *Ind. Manag. Data Syst.* **2019**, *119*, 1457–1491. [CrossRef]
71. Kamble, S.S.; Gunasekaran, A.; Kumar, V.; Belhadi, A.; Foropon, C. A machine learning based approach for predicting blockchain adoption in supply Chain. *Technol. Forecast. Soc. Change* **2021**, *163*, 120465. [CrossRef]
72. Batubara, F.R.; Ubacht, J.; Janssen, M. Challenges of blockchain technology adoption for e-government: A systematic literature review. In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, Delft, The Netherlands, 30 May–1 June 2018; pp. 1–9.