

Post-Quantum Transition in Blockchain Architectures: A Systematic Review of Cross-Layer Security, Performance, and Governance Constraints

Evgeniya Ishchukova ^{1,2,*} , Faezeh Sadat Sajadi ² , Sergei Petrenko ¹, Alexey Petrenko ¹ and Alexey Nekrasov ² 

¹ Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, Sochi 354340, Russia; petrenko.sa@talantiuspeh.ru (S.P.); a.petrenko1999@rambler.ru (A.P.)

² Institute for Computer Technologies and Information Security, Southern Federal University, Chekhova 2, Taganrog 347922, Russia; a2r.sahar@gmail.com (F.S.S.); alexei-nekrassov@mail.ru (A.N.)

* Correspondence: jekky82@mail.ru; Tel.: +7-(928)-1435898

Abstract

We performed a cross-layer, system-level analysis of the post-quantum transition of blockchain architectures through a systematic review. The analysis, based on 108 peer-reviewed studies, moves beyond post-quantum cryptography (PQC) as merely a primitive substitution and examines how quantum pressures cascade through validation, propagation, interoperability, governance, and regulatory layers. Empirical results show that the authenticated payloads for lattice signatures grow from ~65–73 bytes (ECDSA) up to kilobyte-scale sizes, and verification overhead is increased by a factor of $2\times$ to $5\times$ depending on the deployment scenario. Such inflation can narrow block-capacity margins, increase propagation delay under fixed-interval regimes, and shift validator resource thresholds in heterogeneous networks. Moreover, the harvest-now–decrypt-later model creates a temporal asymmetry between the design options and the exposure window. These findings indicate that post-quantum resilience depends more on maintaining a structural balance among the tightly coupled technical and institutional stress channels than on the strength of the algorithm itself, and migration success ultimately depends on the ability to coordinate the management of these constraints, rather than on managing them separately.

Keywords: blockchain security; post-quantum cryptography; quantum threat models; governance; interoperability; migration strategy; architectural resilience; cross-layer security



Academic Editors: Aref Meddeb,
Bacem Mbarek and Arash Habibi
Lashkari

Received: 26 May 2026

Revised: 12 June 2026

Accepted: 15 June 2026

Published: 17 June 2026

Copyright: © 2026 by the authors.
Licensee MDPI, Basel, Switzerland.
This article is an open access article
distributed under the terms and
conditions of the [Creative Commons
Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

For the past decade, blockchain systems have almost exclusively been based on classic public-key cryptography, which includes, among others, ECDSA, ECDH, and hash-based constructions such as SHA-256, to maintain authenticity, non-repudiation, and immutability. These mechanisms have helped to prop up trillions of dollars in digital asset worth and stay secure from classical adversaries. The rapid development of quantum computing, however, brings up fundamental questions of the security of these assumptions. Quantum threat is different from incremental attacks that can often be prevented by a software update or parameter change, and the attacks have the potential to challenge the mathematical hardness assumptions that underline decentralized trust mechanisms [1].

Shor's algorithm would make elliptic-curve and RSA-based systems insecure by allowing recovery of the private key from publicly available data, as shown by systematic

analyses, if a sufficiently fault-tolerant quantum computer is provided [2]. The vulnerability is not a fluke; it is embedded in the structure of blockchain, as addresses and signatures are permanently recorded on-chain. Meanwhile, recent cross-platform benchmarking research indicates that PQC algorithms are not just theoretical but are increasingly being evaluated in real-world deployment contexts within cloud infrastructures and resource-constrained devices, such as [3]. The challenge, therefore, is to evolve from theoretical cryptanalysis to a realistic system-migration problem.

Importantly, the implications of quantum capability extend beyond signature schemes. Blockchain–quantum surveys reveal that the assumption of consensus validation in blockchain, the margin of security, interoperability protocols, and even the process of authentication for blockchain governance are affected by quantum advances [4]. At the same time, PQC surveys in the wider community highlight how migration from classical to post-quantum primitives affects the integration paths for protocols, certificate management infrastructure, and lifecycle processes. These cascading effects are especially intricate in decentralized environments, where upgrades necessitate the agreement of several stakeholders involved instead of some centralized control [5].

In addition to Shor-based key extraction, Grover’s algorithm affects the security of hash functions and the practicality of conducting large-scale searches. While Grover does not break hash constructions, it reduces the security margin by half, which makes the parameters need to be rethought [6].

A further empirical comparison between ML-DSA and a classical implementation of ECDSA also confirms a measurable increase in the size of the signatures and the verification latency for the scenarios for integrating PQC into ECDSA implementations [2,7]. The overheads can vary between the different hardware platforms and, in some cases, can influence transaction throughput and block propagation dynamics, with some reported overheads being around $2\times$ to $5\times$ that of ECDSA depending on the deployment environment; see [8]. While this is not cryptographically impossible alone, it is structurally significant in block-constrained, latency-sensitive distributed systems. Therefore, for assessing the adoption of PQC, in addition to the cryptographic soundness, the operational performance is also crucial [9,10].

Architecture-level implementations support this argument: migrations require changes to authentication flow, time to validate, and resource allocation—especially where decentralized zero-trust models are incorporated. Classical and PQC mechanisms are frequently put forward in tandem as a “hybrid” solution, allowing for a degree of backward compatibility, but this also carries with it its own dangers [11]. Disparities between legacy components and those designed to be quantum-resistant could arise if governance coordination and protocol agility lag behind the cryptographic transition, potentially forming new attack surfaces. This transition thus requires conscious efforts to plan instead of assuming compatibility [12].

One of the defining characteristics of the quantum threat landscape is the harvest-now–decrypt-later (HNDL) approach, where adversaries have the ability to harvest today’s encrypted blockchain data, hoping to decrypt it when cryptographically relevant quantum computers are available [6]. This is especially true for systems where confidentiality and integrity are paramount over long periods, such as digital identity systems, health IoT applications, and financial settlement systems. Therefore, quantum risk assessment needs to consider not only current state-of-the-art computer power but also the progress to be expected in the future [13].

The advent of quantum computing also brings about a greater change in the philosophy of cryptographic design. While classical blockchain security is based on computational hardness assumptions, quantum-native and quantum-assisted primitives examine other

security constructions, such as hybrid and quantum-assisted designs and hybrid constructions [14]. The impact of this development on the migration strategy poses new challenges for blockchain ecosystems, which need to not only identify the post-quantum algorithms they should be using but also how future architectures could incorporate components aided by quantum computing. In this respect, it is both technical and architectural.

Although all these problems have been identified, the literature is still disjointed, with blockchain security surveys providing a comprehensive list of vulnerabilities of smart contracts, interoperability bridges, and consensus mechanisms [15], while a PQC survey categorizes the algorithmic families and summarizes the current process of algorithm standardization. Most of the previous research, however, sees quantum risk mainly as a cryptographic substitution problem. Validators' economic interests, governance issues, regulatory concerns, and constraints on scalability are not typically discussed in a unified framework for deployment analyses [16].

Recent surveys have made significant strides in this area: Fernández-Caramés and Fraga-Lamas list post-quantum primitives suitable for blockchains [17]; Parida et al. systematically survey post-quantum distributed-ledger systems [18]; Yang et al. compare post-quantum and quantum blockchains and mention performance and architectural issues [19]; Ramzan and Cimato list cryptographic options in the quantum era [20]; and Gharavi et al. explore the IoT setting [21]. Early works like Aggarwal et al. [22] estimated the exposure of specific networks to Shor and Grover attacks. However, these works mostly treat scalability, governance, and economic considerations as parallel dimensions rather than as coupled channels. What is under-examined is the system-level interaction between them—how cryptographic overhead cascades through propagation delay, validator economics, governance latency, and regulatory exposure as a single coupled system, and how migration can be sequenced under these joint constraints. A comparison of the present review with the most pertinent previous reviews along these dimensions is presented in Table 1.

Table 1. Positioning of the present review relative to recent post-quantum blockchain surveys (Yes = addressed substantively; Partial = addressed in part; No = not addressed).

Review	Primary Scope	Cross-Layer Coupling	Performance Quantification	Governance Latency	Regulatory Fragmentation	Phased Migration Roadmap
Fernández-Caramés and Fraga-Lamas, 2020 [17]	PQC primitives for blockchain	No	Partial	No	No	No
Parida et al., 2023 [18]	PQ distributed-ledger survey	Partial	Partial	No	No	No
Yang et al., 2024 [19]	PQ vs. quantum blockchains	Partial	Partial	Partial	Partial	No
Ramzan and Cimato, 2025 [20]	Crypto options, quantum-era	No	Partial	No	No	No
Gharavi et al., 2024 [21]	PQ blockchain security for IoT	Partial	Partial	No	No	No
This review	Cross-layer system-level transition	Yes (C1–C5)	Yes	Yes	Yes	Yes (O1–O4; Phases A–D)

However, empirical benchmarking reveals that optimized PQC implementations can be used under specific conditions and achieve tolerable performance. However, there are so few studies that consider performance overhead in combination with consensus dynamics, DAO governance mechanisms, block size limitations, and compliance paths. Regulatory analyses also suggest that quantum readiness could evolve from being optional to mandatory compliance requirements [10,16].

There is, therefore, a lack of general, deployment-focused comparative analysis that simultaneously considers the following:

- Layered quantum threat models;
- Family-level PQC performance and complexity trade-offs;
- Rigidities in migration processes in decentralized governance settings;
- Scalability and energy requirements for post-quantum integration.

To ensure the security, efficiency, and institutional legitimacy of blockchain systems in the coming quantum era, this multidimensional problem must be addressed.

2. Methodology

We use the systematic literature review (SLR) protocol to find persistent and structurally unresolved challenges for blockchain systems in a quantum threat condition. The review is clearly a system-centric review, not just a feasibility review, but one that considers quantum risk in the context of scalability constraints, interoperability, governance coordination, and long-term operational requirements. To be transparent and reproducible, the protocol was based on the identification, screening, and synthesis practices adopted in blockchain-related SLRs and bibliometric reviews in general, which are guided by PRISMA [23]. The structuring decisions and the reporting process for the review were influenced by related blockchain SLRs in adjacent domains [24].

The selection of the studies followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 guidelines [23] and data flow throughout the study selection process is summarized in the PRISMA 2020 flow diagram (Figure 1). The methodological systematic review is not a health-related review but an engineering and computer-science systematic review so was not registered in PROSPERO; therefore, there was no separate protocol published. Screening, eligibility and synthesis were performed based on previously defined criteria in the following Sections 2.3–2.6.

2.1. Review Objectives and Research Questions

The primary goal is to collate evidence of the variety of quantum threats and post-quantum migration pressures experienced at various layers and deployment contexts of blockchains and to pinpoint areas where existing mitigation strategies are partial, fragile, or impractical. The SLR has the following research questions as its pillars (RQs):

RQ1: What are the most-often-referenced threat mechanisms in the blockchain literature that involve quantum (e.g., key-compromising attacks using Shor, hash-margin reduction attacks using Grover, and time-asymmetric HNDL attacks)?

RQ2: What are the impacts on system performance measures (transaction size, validation latency, bandwidth, throughput) of transitions in post-quantum cryptographic techniques (digital signatures, KEMs, hybrid modes) in different deployment scenarios?

RQ3: What cross-layer coupling effects are reported or implied between the adoption of PQC and the blockchain properties of scalability, interoperability, and the feasibility of upgrading the blockchain governance?

RQ4: What methodological and empirical challenges remain in migration pathway assessments for post-quantum networks, especially for the scenarios of heterogeneous node capabilities and transitional hybrid adversary assumptions?

Table 2 shows where each research question is addressed in the rest of the paper.

Table 2. Mapping each research question to the sections where it is addressed.

RQ	Research Question	Section(s) Where Addressed
RQ1	Most-referenced quantum threat mechanisms (Shor, Grover, HNDL)	Sections 3.2.1 and 3.2.2
RQ2	Performance impacts of post-quantum transitions (size, latency, bandwidth, throughput)	Sections 3.1.2, 4.1, 5.2 and 5.3
RQ3	Cross-layer coupling effects (scalability, interoperability, governance)	Sections 3.6 and 4.1–4.3 and Section 5.4
RQ4	Remaining methodological and empirical challenges in migration assessment	Sections 4.4, 4.5, 5.6 and 6

2.2. Data Sources and Search Strategy

The basic question included terms from blockchain, quantum/PQC, and domains at the system level. The final Boolean structure used over the databases (syntax adjusted depending on the indexing engine) was the following: (“Blockchain” OR “distributed ledger”) AND (“quantum computing” OR “post-quantum cryptography” OR “quantum-resistant” OR “quantum-safe”) AND (“security” OR “scalability” OR “governance” OR “interoperability”).

Searches were limited to fields that were available in the database interfaces (title, abstract, and keyword). The indexing engine made syntax changes, and the conceptual structure of the query was the same in each repository. The publication window was from January 2018 to January 2026, and the final search was done in January 2026. Studies published in late 2025 or early 2026 were considered only when they had been formally peer-reviewed and had a DOI at the time they were retrieved.

Google Scholar was mostly used to trace citations and to find more recent publications that are interdisciplinary, from which the peer-reviewed and deduped papers from the primary dataset were retrieved. No citation tracking was done using Google Scholar, and this process was not considered as a separate identification process in the PRISMA screening pipeline.

The search terms were built from three concept blocks: blockchain and distributed ledgers, post-quantum and quantum-safe cryptography, and system-level deployment. For each block, terms were first taken from a set of seed papers in the field and then expanded with common synonyms (for example, distributed ledger and DLT; quantum-resistant, quantum-safe, and post-quantum), so that papers using different wording would still be retrieved. The combined string was checked against a set of known relevant papers to confirm that they were returned, and the final search terms were reviewed and validated by two domain experts before the search was run. This follows established guidance for systematic reviews and mapping studies [23,25,26].

2.3. Inclusion Criteria

The studies have been limited to those that met all of the following inclusion and exclusion criteria so that the corpus could be used for system-level synthesis. The inclusion criteria are:

- Peer-reviewed journal articles or conference proceedings from January 2018 to January 2026;
- Discussions of specific challenges that blockchain may raise, that might have consequences in the system and not just in specific prototypes, but without generalizing to the entire system;
- Constraints in adopting and/or migrating to post-quantum cryptography or direct treatment of quantum computing risk (impact on performance, integration, etc.).

2.4. Exclusion Criteria and Thematic Weighting

The exclusion criteria and thematic weighting are:

- Non-peer-reviewed materials (white papers, blogs, non-scholarly books), reports, theses, and preprints (unless later published in peer-reviewed sources);
- Studies wherein only a specific application scenario was available that might give a limited perspective without being generalizable to whole-system insights;
- Papers in which PQC or quantum risk is mentioned superficially, with only one paragraph of a “future work” statement, without a thorough analytical examination.

These criteria follow established guidance for systematic literature reviews and mapping studies [23,25,26]. Only peer-reviewed journals and conference papers were included, since peer review provides a basic and consistent quality check across a corpus that is meant for system-level synthesis. The window of January 2018 to January 2026 was chosen because the literature that treats post-quantum cryptography as a concrete blockchain concern, rather than a general future risk, appears mainly from 2018 onward, in step with the NIST post-quantum standardization process. Non-peer-reviewed material, reports, theses, and preprints were excluded for the same quality reason, unless a preprint was later published in a peer-reviewed venue.

In addition to applying a bilateral eligibility check, a weighing strategy was employed to evaluate subjects qualitatively, preventing over-representation and potential influence from a narrow stream on the whole subject. This is the same approach that has been implemented in high-quality SLRs to reduce the risk of imbalance in the study contributions, which focuses on the density of the study contributions, rather than the number of published studies on a specific topic [9,27], as detailed in Table 3.

Table 3. Contribution-weighted thematic framework used to guide qualitative synthesis of the included studies ($n = 108$).

Domain	Share (%)	Studies (Approx.)	Research Maturity	Analytical Role
Quantum Threats and PQC	40	45–60	High	Primary cross-layer risk axis
Architecture and Interoperability	25	25–35	Moderate–High	Structural integration constraints
Scalability	20	20–30	Moderate	Performance impact under PQC
Governance and Regulation	10	10–15	Emerging–Moderate	Upgrade coordination limits
Energy and Sustainability	5	5–10	Emerging	Operational overhead context

The indicative evidence density is based on the density of the studies that contributed substantively to the qualitative synthesis, while the density estimates are based on the patterns of retrieval at the database level prior to final screening; these do not correspond with the size of the studies that were included in the final corpus ($n = 108$). Thematic balance was achieved by weights during the synthesis process but not as exclusion thresholds.

Qualitative synthesis and prioritization were driven by weights only, not used as exclusion thresholds. They were not used as an independent exclusion criterion in any phase of the PRISMA-guided screening process but rather were used to guide the thematic emphasis during qualitative synthesis.

2.5. Study Screening and Selection Process

A systematic screening process was implemented in a multi-stage pipeline. The data from the database searches ($n = 234$) were consolidated, and 74 duplicate records were eliminated to obtain 160 unique records. Title and abstract screening was carried out by the lead author against the predefined eligibility criteria using a transparent relevance-scoring protocol, and 33 records that fell below the retention threshold were excluded at this stage. There were 127 studies that were full-text-reviewed. Nineteen studies were excluded after full-text assessment for the following reasons: not blockchain-specific ($n = 7$), purely theoretical without architectural relevance ($n = 4$), non-peer-reviewed technical reports ($n = 3$), and insufficient methodological transparency ($n = 5$).

The study identification, screening, eligibility, and inclusion process from the 234 initially identified studies to the 108 studies included in the analysis is summarized in the PRISMA 2020 flow diagram (Figure 1).

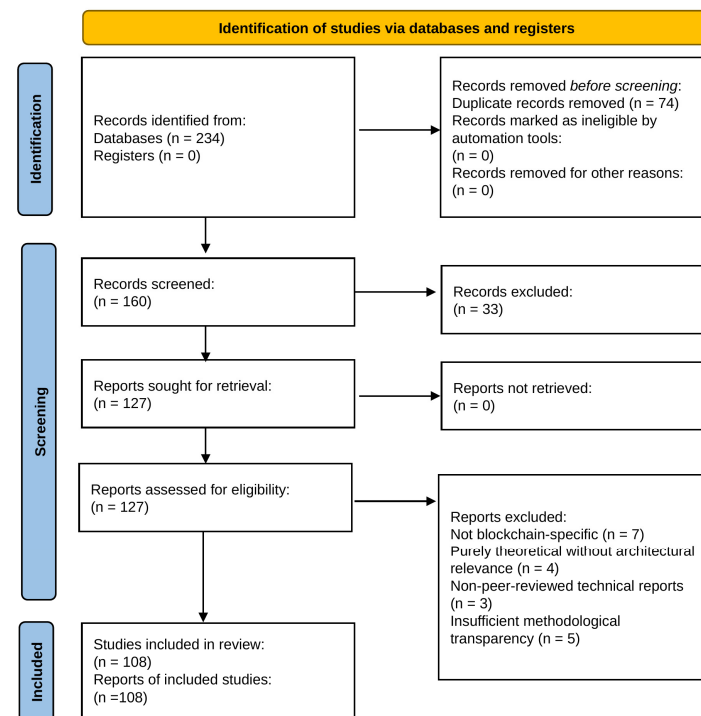


Figure 1. PRISMA 2020 study selection flow (records identified = 234; final included = 108).

A complete screening register, which lists every identified record together with its relevance score under the predefined criteria, is provided as Table S1 in the Supplementary Materials, so that the selection process can be independently audited and reproduced.

2.6. Data Extraction and Synthesis

The following fields were extracted from each included study ($n = 108$):

- Security considerations, including what risks are present on the system, as well as their sources, types, and levels.
- Signature/KEM primitives (classical, post-quantum, hybrid); performance and integration evidence: reported (or inferable) effects on signature size, verification cost, block/transaction format inflation, bandwidth and throughput constraints. A review of the literature about performance claims in PQC benchmarking and implementation informed the interpretation of performance claims across heterogeneous environments [3].
- Explicit or implicit implications for scalability, interoperability, feasibility of governance upgrades, economics of energy/validation, and operational constraints.
- Threat handling, i.e., whether there was a threat model or hybrid threat model assumption.

Qualitative synthesis was performed based on the thematic coding process that was linked to the weighting process (Table 3). The objective was to find failure modes that recur at the system level, cross-domain dependencies, and evidence gaps that align with synthesis patterns used in previous blockchain SLRs [28,29].

Studies reporting heterogeneous metrics (e.g., incomparable platforms or measurement baselines) were not subjected to a pseudo-meta-analysis.

2.7. Quality Considerations and Reporting Discipline

Given this variety in the empirical rigor of blockchain and security engineering studies, each work studied was evaluated in three aspects: (i) clarity of the assumptions, (ii) transparency of the evaluation setup, and (iii) traceability from the claim to evidence. For studies that explored claims of AI/ML-based mitigation or detection, the extraction template also captured whether the study outlined operational constraints such as human oversight, transparency, or governance-related constraints often discussed in the context of responsible AI practice and whether they discussed claims of interpreting security automation relevant to decentralized systems [29].

A total of 108 studies were included, the majority of which focused on empirical benchmarking, prototype implementation, or measurable performance evaluation, while the remaining studies were mostly architectural or analytical.

3. Background and Key Challenges

Blockchains were not created for quantum computing. They were designed around classical hardness assumptions, elliptic curves, discrete logarithms, collision-resistant hashing, and many architectural choices that combined replication, consensus, and economic incentives. Scalability, implementation risks, energy use, and governance conflicts have been the primary concerns for more than ten years. These stressors are not the same stressors of quantum computing; they are stressing together. To be able to analyze quantum risk, it is necessary to understand this amplification, not to consider it as a completely different category [30].

This section, therefore, differentiates classical constraints from quantum-exacerbated dynamics in terms of scalability, security and privacy, sustainability, governance, and regulatory exposure. This is not about drama; it is about understanding how post-quantum migration will change cost structures, the coordination dynamic, and risk horizons [31].

3.1. Scalability Challenges

The biggest engineering challenge in public blockchain systems is still scalability. The literature always shows that the performance metrics of transaction throughput, latency, storage growth, and network propagation are all interlinked and are not independent of each other but are outcomes of the consensus and full replication models themselves used in systems design [32]. Before the quantum factors, public permissionless networks had to balance efficiency and scalability, while maintaining a secure and decentralized network.

To lower confirmation delay and boost parallelism, several innovative approaches have been suggested, such as DAG-based re-construction, sharding, off-chain channels, and committee-based consensus mechanisms [33]. However, these strategies often come at a cost of shifting away from determinism and towards complexity or new coordination surfaces. As well as the classical cryptographic assumptions, the ceilings for scalability were already high.

3.1.1. Classical Scalability Limits

There is empirical evidence showing that the throughput of widely deployed public chains is orders of magnitude smaller than centralized chains for two reasons: First, that cryptography is not expensive, and second, that consensus in adversarial situations requires world-wide agreement. As the block size grows, capacity in the short run increases and propagation delay increases. A smaller block interval will result in a more responsive program but will increase the chance of stale blocks. Sharding makes cross-shard validation challenging but serves to distribute load [34].

Under controlled settings, experimental solutions like Crust Chain have shown the capacity for structural redesign proof and erasure coding that can achieve a throughput of over 1000 TPS [35]. Also, in edge or federated contexts, the communication overhead can be reduced in the case of committee-based architecture in comparison to the classical variants of PBFT [36]. Such improvements are largely reliant on assumptions when deploying, validator homogeneity, and controlled latency environments, however.

A key point is that scalability restrictions come from replication logic and communication costs, which are critical in an adversarial way. Cryptography is a contributor—but not the only determinant [37].

3.1.2. Post-Quantum Amplification Effects

This is altered in some ways during the post-quantum migration. Other signature schemes like Dilithium and Falcon have higher key and signature sizes and verification overhead compared to ECDSA [38] or ARM-based embedded systems when Falcon is used in blockchain authentication flows; signing latency is becoming the biggest constraint [2]. The same applies to the example of Kim et al., where measurable TPS degradation is observed with the use of post-quantum signatures instead of classical signatures, even in the case of an optimized delegated consensus [39].

The effect is not one-on-one. Larger blocks transmit at a lower rate of transactions per block or larger blocks in a heterogeneous network. In permissionless, latency-sensitive applications, greater propagation delay results in greater likelihood of stale blocks. This, in turn, decreases the effective throughput unless block intervals are changed [40,41].

These overheads are even more apparent in embedded and IoT application spaces where memory and energy resources are scarce. To reduce the impact on resources, lightweight post-quantum variants on the primitives of the family of Ascon have been developed, which must maintain security margins while still not compromising performance [42].

The significant thing to note is that post-quantum cryptography does not introduce new categories of scalability. It exacerbates current limitations such as payload growth, validation costs, and propagation delays in the same architectural logic [43].

Table 4 summarizes the main scalability bottlenecks under classical assumptions and shows the interplay of post-quantum cryptographic overhead with each of these. The table does not seek to estimate the magnitude of impacts but rather attempts to identify the most important mechanism by which post-quantum migration alters existing constraints.

Table 4. Mechanistic interaction between classical scalability bottlenecks and post-quantum cryptographic overhead.

Scalability Bottleneck	Classical Driver	PQC Amplifier	Primary Metric	Net Effect
Transaction Throughput	Block size limit + consensus delay	Signature size inflation (Dilithium/Falcon)	TPS	Reduced tx density per block or increased payload
Propagation Delay	Network latency heterogeneity	Larger block payload	Block interval stability	Slower dissemination increases stale probability
Validation Overhead	Signature verification cost	Heavier lattice verification	CPU/Memory	Increased per-tx verification cycles
Storage Growth	Full replication	Larger signatures persist on chain	Ledger size	Accelerated state growth
Consensus Communication	Quorum messaging	Larger authentication payload	Bandwidth	Increased message size per round

As presented in Table 4, the major impact from post-quantum integration is not architectural, but rather parameter stress. Even in permissionless networks, the block size,

propagation dynamics and verification cost were already limiting factors [40]. The major change in the way that post-quantum signatures will be used is their operating margin, especially in latency-critical and resource-constrained environments. This distinction is crucial: the scalability issue stays the same, but its tolerance levels become more restrictive [4].

3.2. Security and Privacy Challenges

Security covers cryptographic primitives, consensus integrity, smart contract execution, and the resilience of the network. Layer-oriented surveys reveal vulnerabilities spread throughout the entire architecture's layers, such as key management issues, consensus manipulation, and contract-level bugs [15].

If these assumptions are true, Byzantine fault tolerance and economic incentives keep the integrity of the ledger. However, security issues like smart contract vulnerabilities, cross-chain bridge exploits, and governance manipulation continue to be common [44].

Another stress is privacy. Unlike anonymous systems, public blockchains are pseudonymous. Address reuse, clustering techniques, and metadata correlation allow behavioral linkage. Some risks are reduced by privacy-preserving technologies like zero-knowledge proofs, threshold cryptography, and confidential transactions, but at the expense of computational complexity [45,46].

3.2.1. Classical Threat Surfaces

In classical adversaries, security issues are mostly implementation-related or incentive-related ones. Substantial losses have been suffered due to smart contract exploits, oracle manipulation, and bridge vulnerabilities. In networks that are not sufficiently decentralized, consensus attacks like 51% scenarios are still a theoretical risk [47].

In many mainstream deployments, zero-knowledge constructions and commitment schemes are used to achieve better confidentiality and rely on discrete-log or pairing-based assumptions. The feasibility of homomorphic encryption and integration of ZKP in decentralized learning systems is shown, but these methods cause a non-trivial computation overhead [48].

Therefore, blockchain systems are secured according to layered security assumptions that must be met simultaneously, even where there are no quantum adversaries.

3.2.2. Quantum Threat Models and Temporal Risk

The adversarial model is changed by quantum computing when classical hardness assumptions are weakened. In theory, Shor's algorithm will break both RSA and elliptic-curve cryptography when scalable, fault-tolerant quantum computers are available. The security parameters of symmetric primitives are decreased by Grover's algorithm [49].

Most importantly, current NISQ-based hardware devices do not yet pose a systemic risk—with experimental implementations demonstrating significant degradation in performance as the number of qubits grows [50]. The threat model is temporal, however. The “harvest-now–decrypt-later” scenario assumes that the data on the blockchain will be encrypted today but will be decrypted at some point in the future when quantum computing power is realized [35].

In contrast to many classical attacks, this temporal asymmetry would allow an adversary with a well-developed quantum computing capability to gain unauthorized access to transactions in a signature-based system, to bind an identity to a malicious transaction, and to manipulate the stakes in a proof-of-stake system [37]. For governance mechanisms that are based on the voting integrity lattice or are identity-based, key extraction may directly impact voting integrity.

Hybrid quantum-safe cryptosystems based on the combination of QKD and PQC show resilience but are limited in terms of scalability in authentication [51]. There are also

post-quantum ring signature schemes like Chipmunking that achieve better performance in the anonymity sets but still generate larger signatures than their classical counterparts [38].

Therefore, it is not correct to assert that quantum computing opens new categories of threats. Rather, it increases the severity, reversibility, and time horizon of cryptographic compromise [30].

To illustrate this difference between structural continuity and threat amplification, Table 5 compares quantum to classical threat surfaces at selected architectural layers. Focus is placed on conditional amplification, which is the amplification of existing vulnerabilities, not new ones, by quantum capabilities.

Table 5. Classical threat surfaces and their conditional amplification under quantum adversaries.

Threat Surface	Classical Manifestation	Quantum Amplification	Conditional Scope
Digital signatures	Key compromise via classical attack	Shor-enabled key extraction	Once scalable fault-tolerant QC emerges
Hash integrity	Collision resistance	Grover reduces effective security margin	Requires quadratic speedup context
Proof systems (discrete-log-based)	Assumption failure	Quantum breaks DLOG/pairing-based ZKP	Applies to pairing-based SNARK families
Stake-weighted consensus	Key theft risk	Stake capture via signature extraction	Identity-bound systems
Long-term confidentiality	Data retention risk	Harvest-now–decrypt-later	Time-asymmetric exposure

As shown in the table, most quantum-induced risks materialize only when scalable, fault-tolerant quantum computation is available. This shift from classical to post-quantum security is not a binary switch but a change in the temporal distribution of risk, especially for systems where on-chain data and identity are persistent and consensus relies on identities [41,52].

3.3. Energy and Sustainability

Mining intensity and electricity usage are significant problems pointed out in systematic reviews of proof-of-work systems [32]. Other consensus models (proof-of-stake, reputation-based variants of PBFT) consume less energy but add concentration risks [53].

Post-quantum cryptography operates at a different level. The longer the verification cycles and the larger the signature, the more CPU time and memory are required [53]. This can increase per-transaction energy consumption in constrained environments. The lightweight post-quantum hashing proposals aim to decrease the amount of computation required while maintaining security margins [54].

It is important to note that analyses of sustainability consider energy use as an integral part of consensus structure, node heterogeneity, and deployment scale [55]. Without considering these structural variables, the introduction of new primitives for post-quantum cannot be done without a risk of incremental inefficiency. However, if the model is rebuilt to incorporate PQC, for example delegated proof–luck models, the cost of this can be mitigated to some extent [39].

The sustainability implication is complicated. Migration to post-quantum may lead to higher energy consumption per transaction, but the system-level energy consumption is determined by the energy consumed by the consensus mechanism and the configuration of the network [39].

3.4. Governance Constraints

The issue of governance is yet another tension between decentralization and coordinated decision-making. DAO dynamics studies show that voters' apathy, power concentration,

and coordination inertia are persistent [56]. Even in a classical threat model, protocol changes are hard to get consensus on. This coordination problem becomes worse when it is quantum migration.

To switch to post-quantum primitives, cryptographic upgrades must be coordinated among nodes located in different parts of the world [51]. Cryptographic migration is different from optional feature updates in that it impacts the underlying trust layer.

If scalable quantum attacks materialize, a delay in governance response to a quantum attack may have systemic impacts. However, the negative performance impact and compatibility issues of acting prematurely cannot be overlooked. Strategic roadmaps highlight incremental replacement and crypto-agility instead of sudden replacement [57].

Governance, therefore, becomes a temporal risk management process. The challenge is not just choosing the right algorithms but getting stakeholders, validators, and developers on board with the timing of the transition [58].

3.5. Regulatory and Compliance Pressures

There are two interrelated overlap dimensions between regulatory uncertainty and quantum risk. First, legal systems are increasingly considering forward-looking security obligations. In foreseeable situations, if the cryptographic standards are known to be vulnerable, operators would have an exposure to liability [30].

Second, standardization bodies and industry consortia will likely require critical infrastructure sectors to be post-quantum-ready [59]. More general legal scholarship highlights the necessity of rules and regulations that can accommodate the assumption-changing nature of quantum-enabled security challenges [60].

Compliance is complex with cross-border blockchain deployments. Nodes might be running across jurisdictions, and jurisdictions may have different data protection and encryption standards, which may cause compatibility issues when migrating nodes into different jurisdictions at different times [61].

This means that there is compliance pressure beyond cryptographic implementation [62], driven by quantum. It impacts on certification, liability assignment and cross-jurisdictional interoperability.

3.6. Interdependencies Among Challenges

The challenges listed above do not happen in isolation. The relationship between decentralization and scalability, decentralization and governance resilience, governance and upgrade timing, upgrade timing and regulatory exposure, and all of these are moderated by the cryptographic performance [35].

Consequently, there may be a rise in block propagation delays, which has an indirect effect on stale-block rates and economic incentives, because of signature inflation. The costs associated with validation could increase the likelihood that more resources are invested by the more successful nodes, thus impacting the balance of governance. Longer migration means more exposure to harvest-now–decrypt-later risk [32].

These interactions are systemic, and thus post-quantum migration should not be considered as a substitution problem for cryptography; rather, it should be seen as an adaptation process across layers.

Section 4 will go further in this mapping by focusing explicitly on coupling mechanisms, such as the network-dynamic coupling between signature size inflation and effective throughput degradation with fixed protocol parameters.

4. Cross-Layer Propagation Model

4.1. Architectural Stress Channels

Shor-type attacks are made against public-key schemes in blockchain systems used for authentication and ownership [2]. Meanwhile, the security margins used in symmetric-key and hash-based constructions are degraded by Grover-type speedups [63]. However, the architectural impact of quantum computing is not limited to the cryptographic layer alone [64]. In production blockchain systems, a small number of primitives are used simultaneously across several different subsystems, including transaction authentication, identity binding, consensus validation, cross-domain validation, privacy overlays and governance operations [45]. These primitives are collocated at shared dependency points; therefore, making changes to these elements does not simply shift the security burden to another part of the architecture, but rather spreads it out [59]. Hence, it is most beneficial to think of quantum risk as a cross-layer stressor, and not as one cryptanalytic event.

To explicitly structure this propagation, Figure 2 breaks this up into two steps: first, into the five architectural stress channels (C1–C5) and then into the effects of the subsystems. Channels are used to model the propagation of change and assumptions by the system.

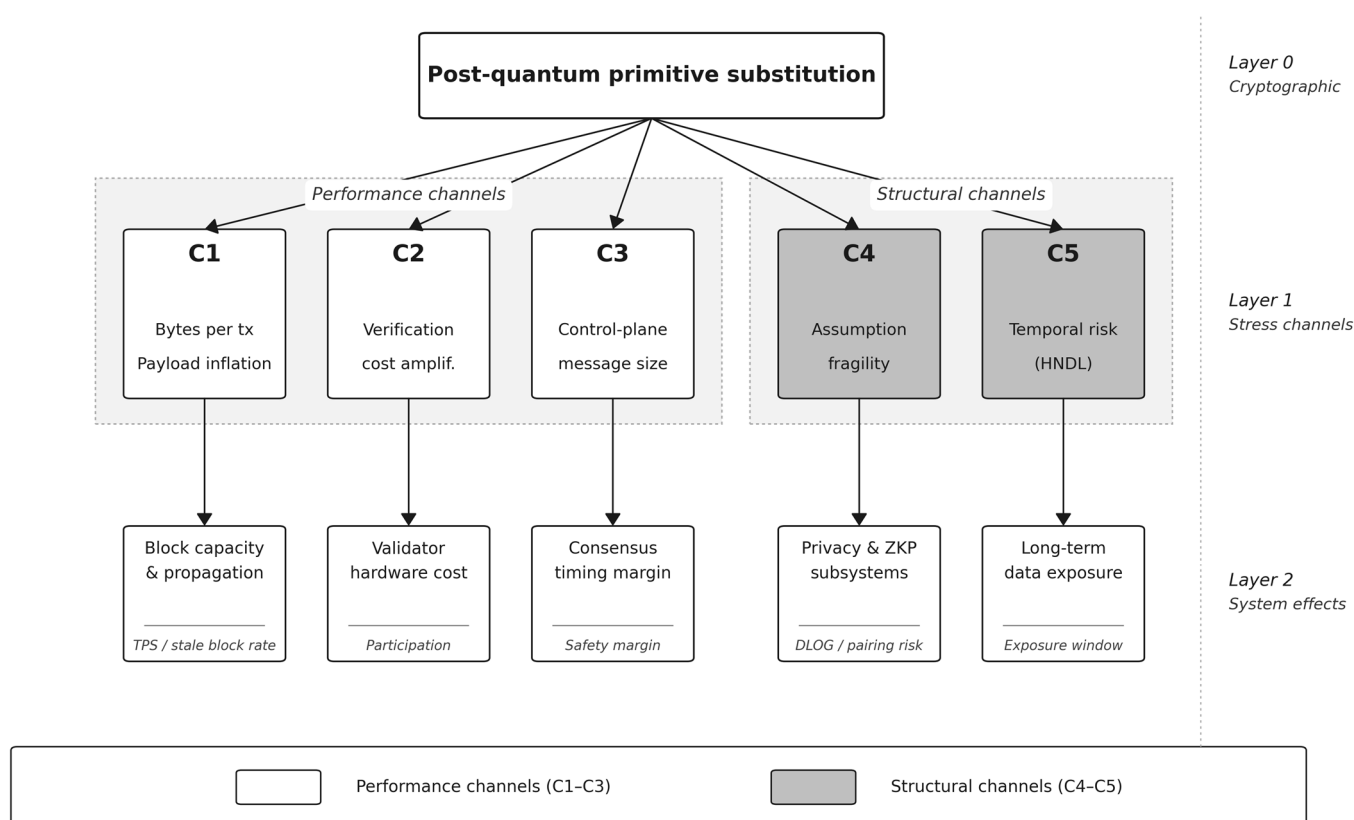


Figure 2. Cross-layer propagation of post-quantum architectural stress channels (C1–C5).

The C1 channel (bytes per transaction) is the clearest in transaction authentication. Today's public blockchains use small elliptic curve signatures (≈ 65 – 73 bytes for common Bitcoin and Ethereum implementations). At first-order structure level, the immediate effect of these can be represented as signature size entering the kilobyte regime with the introduction of NIST-standardized post-quantum schemes like ML-DSA or SLH-DSA:

$$\text{Propagation delay} \approx (\text{payload size} / \text{effective bandwidth}) + \text{baseline latency}.$$

In a heterogeneous network setting (such as the permissionless network) longer payloads lead to longer dissemination times. This, in turn, leads to a reduction in the safety margins between the block interval and propagation delay, which in turn impacts consensus timing [40]. New protocol rules are not needed for the mechanism; it follows the already established protocol building and dissemination mechanisms [65].

The second channel, C2 (verification cost), differs from byte inflation; the arithmetic profile and memory usage of post-quantum signature verification, especially lattice-based schemes, are different from elliptic-curve schemes. Block processing time can be simplified as:

$$\text{Block processing time} \approx \sum_i \text{verification time}(tx_i) + \text{protocol overhead}.$$

With fixed consensus timing, the higher the cost of verifying each transaction, the lower the effective throughput or the higher the minimum hardware requirements for validators. In actual use, this pressure is not limited to transaction validation but also applies to privacy layers and cross-chain verification, where signatures and proofs are repeatedly validated. Participation costs move within the network, but the network remains functional.

The third channel is C3 (control-plane message size), which is not at the transaction payload layer but on the transport or consensus coordination layer. Not every post-quantum primitive has an impact on per-transaction authentication. For example, ML-KEM is mainly responsible for handshake procedures and the establishment of secure channels. In such circumstances, the relation of interest is the timing stability instead of the block payload:

$$\text{Consensus safety margin} \approx (\text{block interval} - \text{propagation delay}).$$

The larger the control-plane and consensus-layer messages become, the longer it takes them to propagate and the less the safety margin, assuming fixed timings. C3 is clearly distinct from C1 to prevent over-claiming the impact on block space, yet recognizes the impact on dissemination stability at the structure level [66].

In addition to performance channels, there are two other limiting factors in migration. C4 (assumption fragility) defines the dependence between security for the subsystems and the dominating hardness assumption of the primitive in the subsystems. For a privacy proof system and a commitment scheme, or an identity-binding system, based on quantum algorithms that attack the discrete-logarithm or pairing-based assumptions, subsystem security is time-conditional [40]. This does not mean all subsystems are not capable of quantum; it highlights those that have quantum-sensitive dependencies from their base primitives.

Lastly, C5 (temporal risk) models the asymmetry caused by harvest-now–decrypt-later models. Exposure can be approximated as

$$\text{Exposure window} \approx (\text{data longevity} - \text{migration completion time}).$$

When the life span of confidentiality is greater than the life span of cryptographic migration, there is a window of exposure if it is non-zero. There is asymmetry, but its size is driven by data retention patterns and upgrade coordination and so is structural [67].

Table 6 is a comparison of stress profiles between primitive classes, but it does not show how these stresses are cascaded into a live system. Figure 2 thus moves from comparing categories to structurally propagating the stress channels (C1–C5) to the downstream subsystem constraints.

Table 6. Architectural stress profiles by post-quantum primitive class.

Primitive Class	Typical Signature/Ciphertext Size (Relative to ECDSA)	Per-Transaction Byte Pressure	Verification Cost Pressure	Network Propagation Sensitivity	On-Chain Storage Persistence	Handshake/Transport Impact	Overall Architectural Stress Pattern
Classical ECDSA (Baseline)	1× (≈ 65 – 73 -byte signature)	None (reference baseline)	Low	Low	Low	Low	Low
ML-DSA (FIPS 204)	≈ 2 – 3 kB (≈ 30 – 45 × ECDSA baseline)	Bytes + verification	High (kB-scale signatures per transaction)	Moderate to high (lattice arithmetic per verification)	High in latency-sensitive permissionless networks	High (large signatures persist in ledger state)	None (not used for transport)
SLH-DSA (FIPS 205)	≈ 8 – 30 kB (≈ 100 × + ECDSA baseline depending on parameter set)	Byte-dominant	Very high (multi-kB signature per transaction)	Moderate (hash-based operations)	Very high (dominates block-capacity margins)	Very high (signatures permanently stored)	None
ML-KEM (FIPS 203)	Ciphertext ≈ 800 – 1200 bytes (handshake context only)	Message-size (transport layer)	None (no per-tx effect)	Moderate (encapsulation/decapsulation cost)	Low to moderate (depending on channel churn)	None (no ledger persistence)	High (node-to-node secure channel overhead)

The diagram is not a performance but a reading guide for the structure. The impact of each arrow is dependent on the implementation choices, but the direction of constraint propagation is inferred from the protocol timing relations, verification aggregation relations, cryptographic assumption inheritance relations, or the migration latency asymmetry relations.

These couplings can be summarized concisely: there are three performance channels, (i) effects of the number of bytes per transaction on block capacity and fee dynamics, (ii) effects on the resources a validator needs to verify transactions, and (iii) effects on the message size of the control plane, which impacts the timing stability. There are also two structural channels: (assumption fragility) and (temporal exposure). This separation is used to avoid the separate architectural pressures converging into one idea of overhead [11].

4.2. Structural Interdependence Under Post-Quantum Constraints

The second dimension in post-quantum migration is energy consumption. The following arithmetic operations and memory accesses are usually more complex in post-quantum signature verification compared with classical elliptic-curve signature verification [7] (ECV).

When the size of the transaction (C1) and verification cost (C2) grows, the use of energy becomes a first-order participation constraint, especially in the case of validators with commodity computers or limited resources. Empirical evaluations show that deployment is still possible, but the resource profile shifts, CPU cycles, memory footprint, and energy budgets become constraints to provide the same level of security guarantees [65].

Studies also demonstrate a connection between “security achieved” and “system unchanged” in an implementation-based capacity. Post-quantum verification can be performed with the help of smart contracts, modified clients, or precompiled modules [3] in EVM-compatible environments. Cryptographic substitution is not an algorithmic upgrade but a protocol-engineering choice with implications for the economics of gas, latency of validation, and validator workload when all is considered [43].

Another element of structural sensitivity is privacy subsystems. Most of the zero-knowledge and commitment constructions used in the deployed protocols are based on discrete-logarithm or pairing-based assumptions, so fall into the quantum-sensitive class identified in C4. Some systems fail to be quantum, but some construction families are quantum because they are based on assumptions that are hard. In privacy-specific blockchain systems, migration pressure is always considered a design selection rather than a secure/insecure binary choice [52].

Some of the dynamics come to a head when focusing on cross-chain interoperability. There are already complex verification pathways in operation, such as bridges and

relay mechanisms. As cross-domain messaging payloads grow (C1) and verification costs increase (C2), latency and operational overhead can increase. The effect is conditional: post-quantum primitives can increase verification costs, and in high-complexity bridge settings, this overhead can exacerbate existing fragilities, unless interoperability designs can reduce duplication of trust and verification [68].

Most importantly, these stress channels are not all present in the blockchain architectures. How C1–C3 pressures manifest as constraints at the system level is subject to differences in block interval, assumptions about validator hardware, execution semantics, and differences in governance rigidity. A kilobyte-scale signature increase can be acceptable for throughput-optimized architecture, but not for conservative block size regimes. Likewise, the burden of higher verification costs could be taken up by homogeneous validator sets, but it would have a tangible impact on participation in permissionless heterogeneous networks [36,69].

This is why stress-induced post-quantum should be considered relative to other blockchain design baselines and not in an absolute fashion. Table 7 is a qualitative comparison of the different blockchain architectural design types and how they are likely to experience C1–C3 pressures when operating in their baseline assumptions regarding timing, execution, and validators. The intent here is not to compare different networks, but rather to highlight that the same post-quantum primitive substitutions can result in different stress profiles as a function of block interval regimes, propagation margins, validator heterogeneity, and governance rigidity.

Table 7. Qualitative comparison of architectural sensitivity to post-quantum stress channels (C1–C3) across representative large-scale blockchain design types.

Architecture Type	Block Timing Regime	Validator Heterogeneity	C1 Byte Sensitivity	C2 Verification Sensitivity	C3 Propagation Sensitivity	Governance Rigidity	Overall PQ Migration Difficulty
Large-Block PoS Public Chain	Moderate interval, high capacity	High	Moderate	Moderate–High	Moderate	Moderate	Moderate
Short-Interval PoW Chain	Short interval, tight propagation margin	High	High	Moderate	High	Moderate	High
Committee-Based Permissioned Chain	Flexible interval, bounded membership	Low–Moderate	Low–Moderate	Moderate	Low	High (institutional)	Moderate
DAG-Based/Parallelized Architecture	Asynchronous or semi-asynchronous	High	Moderate	High (parallel validation load)	Moderate	Moderate	Moderate–High
Layer-2/Rollup-Centric Ecosystem	Off-chain batching dominant	High (operator-dependent)	Low (on base layer)	Moderate	Low–Moderate	Moderate	Low–Moderate

This comparison focuses the analysis on the patterns of sensitivity at the architecture level (Table 6), rather than the primitive-level characteristics of stress, making it easier to understand the byte inflation, verification amplification, or propagation instability that will most likely be constraints.

How stress channels propagate between various system baselines depends on a combination of post-quantum migration architecture, primitive selection, verification placement, and execution semantics, as shown in Table 7. To convey these interdependencies, cryptographic migration is treated as architecturally neutral and then compared through the lens of channels to find where and how it is likely to become binding for mitigation efforts [70].

4.3. Governance and Regulatory Fragility Under Quantum Threats

Governance and regulatory mechanisms are a control layer that are built on top of protocol execution but are directly reliant on cryptographic stability. In classical threat models,

governance vulnerabilities usually take the form of delays in coordinating upgrades, disproportionate voting power, reduced participation, or problematic upgrade procedures [16]. These tensions can be ongoing but do not generally jeopardize the cryptographic integrity of previously agreed conclusions.

A quantum threat model alters the nature of the temporal structure of risk. The speed at which cryptographic assumptions might erode and the slower pace of collective decision-making and standards development are decoupled [58]. The time it takes for a governor to notice a risk, decide to issue a standard to mitigate it, then make it available across the network can thus be considered governance latency; the latter is complicated by the fact that post-quantum migration may involve changes in transaction formats and verification rules, rather than just updates to the parameters [71].

Analysis of empirical evidence from blockchain upgrade processes shows that the typical protocol upgrade for large public networks has taken several months in the past, with coordination typically involving client implementation, validator signaling, and exchange compatibility [70]. When cryptographic primitives are used to support identity binding, staking, and governance of the treasury, this coordination latency is directly related to the length of the hybrid cryptographic exposure [58].

The effective exposure period is not only limited by quantum-capable timelines but also by the speed of governance responses [37] if the transaction format needs to be altered or some consensus rule is to be activated for post-quantum enforcement. In this respect, governance delay is a multiplicative rather than neutral administrative variable acting on temporal risk.

Decentralized autonomous organizations (DAOs) make the coupling explicit. Voting, treasury control and identity binding are based on digital signatures which are presumed to be durable over long time horizons [72]. If signature schemes should be proven vulnerable to scalable quantum key extraction, then the proof of previous governance actions becomes conditional [38]. Multi-signature and threshold constructions can solve this single-key fragility, but if it is based on elliptic-curve primitives, then it also suffers their same fragility class [15].

This raises the question of retroactive governance risk—actions taken based on “classical hardness” assumptions can be challenged once key recovery becomes possible. The risk is related to quantum timelines, but the structural exposure is there, because of the long-term nature of governance artifacts, and because they are publicly verifiable [13]. Systematic impact would be both by the exposure of the cryptographic system and by the acceptance of retroactive reinterpretation by the institutions [58].

Governance latency is not an abstract problem, as has been seen in the time it takes for protocol upgrades to be executed, even when not controversial and well-funded. The Schnorr/Taproot change was proposed to the developer’s mailing list in May 2019 and completed as BIPs 340–342 in January 2020 [73], but was not activated until November 2021, and it is the first consensus change since SegWit in August 2017 [74]. The transition to proof-of-stake ran a separate Beacon Chain from December 2020 that only merged with the main chain in September 2022 [75] after years of research and repeated delays. They were all upgrades that were optional and generally very useful, but each required years of coordination. This is a mandatory, critical security move; it affects the signature scheme that secures all accounts and historical records, and the governance latency is likely to be as long and difficult to compress, if not longer.

A second fragility channel is added through regulatory systems. Blockchain networks function in jurisdictions of different legal attributes, and quantum risk is global and non-localized by technology. With the advent of post-quantum readiness in cybersecurity evaluations, regulators could require a minimum level of cryptographic security for infrastructures

with long-lived or sensitive data [76]. But regulatory adaptation is not always consistent, leading to compliance fragmentation between areas.

Regulatory responses work in a formal compliance cycle, which may take longer than technical patch deployments, unlike protocol-level coordination. In cryptographic adequacy standards that are built into financial reporting or digital identity standards (e.g., jurisdictions that include cryptographic standards in their certification or digital identity standards [16]), delayed quantum-readiness alignment may expose operators to dual-layer risk: technical vulnerability and regulatory non-compliance [77].

The effective regulatory lag can thus be described as the period between publishing the standard, the interpretation by the supervisor and the date the compliance is made enforceable [78]. If blockchain systems span several jurisdictions, this time lag becomes non-uniform and adds to the pressure of compliance in a way that can lead to uneven time schedules for the deployment of upgrades, instead of making them uniform [31].

Instruction-wise, using a harvest-now–decrypt-later model makes the evaluation process more complicated. When compromise occurs years after deployment, the assessment of security posture will be measured not just by what has happened in the past, but by transition management decisions [37]. Governance latency and regulatory asynchrony may then cascade slow coordination, delay mitigation, and regulatory uncertainty about the possible costs or interoperability issues if early adoption further discourages it.

This regulatory delay is not consistent throughout jurisdictions, and the differences in delay are one source of fragmentation. The United States has already enacted binding deadlines for national-security systems based on NSA CNSA 2.0 [79] and finalized NIST standards [80–82], and the EU [83] and UK [84] have recommended roadmaps that have an endpoint of 2035; China is choosing its own algorithms instead of the NIST suite [85]. A blockchain that works throughout these regimes is thus subject to multiple migration clocks, some required, some recommended, and in China’s case a different cryptographic target. These regimes are summarized on the most relevant dimensions for blockchain migration in Table 8.

Table 8. Regulatory regimes for the post-quantum transition across major jurisdictions, compared along the dimensions most relevant to blockchain migration.

Jurisdiction	Reference PQC Standard(s)	Binding Timeline	Approach	Sectoral Focus	Blockchain-Migration Implication
United States	NIST FIPS 203/204/205; NSA CNSA 2.0 for national-security systems	Yes—CNSA 2.0 milestones; full transition by 2035	Mandatory (NSS); statutory planning for civilian agencies	Federal government, national-security and defense systems	Procurement and TLS requirements cascade to vendors; ECDSA deprecated 2030–2035
European Union	NIST standards referenced; hybrid (PQ/T) recommended	Recommended—high-risk by 2030, full by 2035	Advisory roadmap, binding via CRA, NIS2, DORA	Critical infrastructure, finance, digital products	Crypto-agility and bill-of-materials duties reach DLT financial infrastructure
China	Sovereign SM-series; own PQC via the NGCC program (not NIST)	Not yet defined—selection ongoing; standards expected ~2028–2029	Mandatory commercial-cryptography regime; PQC pending	Commercial cryptography; finance and energy prioritized	Sovereign primitives create a cross-border interoperability split
United Kingdom	Endorses NIST PQC (ML-KEM, ML-DSA, SLH-DSA)	Recommended—three phases (2028/2031/2035)	Advisory (NCSC guidance)	Critical national infrastructure, finance, government	Same 2035 endpoint; harvest-now–decrypt-later exposure for long-lived ledger data

4.4. Limits of Incremental Mitigation and Piecemeal Approaches

While scalability, security, and decentralization are all desired properties of migration to post-quantum cryptography, they are bound by a trade-off that limits their practical implementation. The incremental substitution, which is to replace one signature scheme without changing other parameters, does not affect the system equilibria, but it also does not produce immediate disruption [38]. However, in blockchain applications, comparative

studies of post-quantum signatures consistently demonstrate that as the performance overhead of the signature grows, the cost of validation grows, even as the number of transactions per second and the number of participants in the blockchain increases, while maintaining the same cryptographic security goals [10].

As a result, as the block size increases to accommodate larger signatures, propagation delay grows, and validator resource needs increase. If limits are unchanged, transaction density decreases, which impacts throughput and fee dynamics [86]. Likewise, increased verification overhead can be paid for with more powerful hardware assumptions or with flexed timing parameters, but neither of these changes removes participation constraints from the protocol [77].

These patterns suggest the interplay between post-quantum cryptography and architectural baselines that rely on compact elliptic-curve primitives [49]. The additive patch mentality in the context of quanta may be a mistake because of the dependencies identified in C1–C3. These system-level migration frameworks focus on coordinated migration from one format to another, from one verification location to another, from one aggregation method to another, and from one point of governance to another, instead of algorithm replacement in isolation [9,87].

4.5. Persistent Challenges and Research Gaps

Interventions in one subsystem often result in a change in tension rather than resolving the system's tension. While post-quantum authentication offers improved long-term robustness, it can also lead to higher payload and verification costs per transaction, impacting block capacity and validator resource usage, respectively, which in turn raises its requirements [37]. These pressures correspond to observations made in actual prototyping and comparative performance experiments of post-quantum blockchain systems.

The inverse situation also exists for subsystems of privacy. If zero-knowledge and commitment constructions rely on discrete-logarithm or pairing-based assumptions, the migration pressure is extended to the proof systems and authentication logic used in the system, as in [88]. When choosing quantum-robust constructions, the computational overhead and integration complexity may be higher compared to traditional constructions.

Feasibility is also affected by energy and hardware constraints. Evaluation on constrained or heterogeneous platforms shows that deployment is feasible, with observable changes and a measurable impact on CPU utilization, memory footprint, and energy profile of the primitives [3]. These changes affect the participation of validators and their expense structure, not just cryptographic correctness.

Structural persistence is added by governance and regulatory domains. Layered cryptographic stacks and crypto-agility are the recurring themes in transition strategies for post-quantum cryptography, which attempt to deal with extended periods of hybrid mode [89]. During such periods, layered cryptographic stacks and backward-compatibility mechanisms reduce immediate exposure but increase system complexity [18].

The pressures recur across architectural contexts as illustrated in Table 7 and this aids in the identification of the remaining directions of research.

The general meaning is methodological. However, a naïve assessment of post-quantum transition using algorithmic security or per-algorithm performance metrics is not enough [43]. System-level assessment must also incorporate security margins, transaction-format overhead, propagation dynamics, validator cost profiles, and governance responsiveness and regulatory exposure, and be explicitly made conditional and temporal with respect to quantum risk [67].

The C1–C5 channel model is analytical and synthesis-driven and was based on recurring patterns of structural elements that were found across the literature reviewed. It is

not an experimentally proven performance model nor based on controlled measurements across deployments in a live blockchain. Instead, it offers a conceptual stress-mapping model to explain the flow of post-quantum substitution stress through architectural layers.

5. Post-Quantum Migration as a Constrained Architectural Transition

Section 4 showed that pressures from the quantum era do not stop at the cryptographic primitive but are carried up to the validation, propagation, interoperability, and governance layers. Migration to post-quantum security should hence be seen as a constrained architectural transformation and not as a primitive replacement exercise [19,20]. When considering post-quantum assumptions, cryptographic selection, performance containment, validator participation, interoperability alignment, and governance feasibility are becoming self-serving variables.

This section consolidates those constraints into a structured migration logic.

5.1. System-Level Design Objectives Under Cross-Layer Coupling

As mentioned earlier, in post-quantum scenarios there are correlations across layers of the cross-layer design regarding cryptographic durability, validation cost, propagation latency, and governance coordination [21,90] that prevent these aspects from being tuned individually. Migration decisions must therefore concurrently meet structural goals.

O1. Cryptographic Durability Across Temporal Exposure

The harvest-now–decrypt-later model is a time-asymmetric model in which data collected under classical assumptions can be used once scalable quantum capabilities emerge [54]. For systems that manage persistent identities, treasury allocations, or governance artifacts, forward security for new transactions is insufficient.

Durability therefore includes: (i) reliance on standardized primitives selected through the NIST process (ML-DSA, ML-KEM, SLH-DSA) to ensure evaluation maturity and ecosystem readiness [71]; (ii) identification and treatment of legacy signatures and ciphertexts in historical state; and (iii) governance processes for revalidation, archival treatment, and deprecation of quantum-vulnerable artifacts. Research on quantum exposure in critical infrastructure highlights the importance of “codesigning” and certificate processes as high-priority transition areas in quantum risk, which further emphasizes the importance of treating codesigning and certificates as a lifecycle process and not just a forward-only one [91].

Durability is therefore a property of the lifecycle of the ledger, and not just a property of primitive-level guarantees.

O2. Performance Containment under PQC Overhead

As described in Section 4, validation and propagation channels in blockchain systems are consistently found to suffer from significant increases in signature expansion and signature verifier costs for NIST candidate signatures in empirical evaluations [50]. The concept of a “defensible objective” is not to preserve classical throughput, but instead it is to limit degradation within decentralization-preserving bounds.

At an architectural level, the challenge is not superficial, but structural, and prototype post-quantum blockchain architectures prove that aggregating signatures, particularly segregated-witness patterns, can help plug those payload size holes if added at the design level, instead of as a retrofit [92]. Asynchronous frameworks or redesign-oriented frameworks also make performance containment a part of the consensus logic design, not an addition to it [93].

Thus, performance is considered as a boundary and is not regarded as an optimization objective without taking security into account.

O3. Validator Inclusiveness under Resource Asymmetry

Studies on integration in the IoT, medical, and industry domains reveal that PQ overhead is more severely impacted in resource-limited networks [70,94]. An absence of architectural constraints can mean that greater verification costs can benefit well-provisioned operators, which may lead to an indirect increase in governance concentration risk [66].

Inclusiveness, thus, needs to be feasible in diverse hardware environments and without mitigators that give rise to implicit trust concentration. Consensus-layer proposals that include post-quantum resilience also stress the need for decentralization to not only be maintained but preserved during the transition [95]. The explicit migration constraint is thus validator symmetry, (e.g., keeping the resources required by validators similar across validators).

O4. Interoperability and Governance Compatibility

Committee relays, threshold validation, or light-client verification models are common models for interoperability frameworks [96]. In the post-quantum blockchain security context, concentrated or single-chain cryptographic checkpoints are considered systemically amplified. Surveying the security of post-quantum blockchains highlights the importance of strengthening primitives at the single-chain level while preserving cross-chain fragility that relies on classical or concentrated assumptions [19].

Migration should therefore ensure compatibility with privacy-preserving subsystems [54] and ensure that all cross-chain authentication is quantum-safe, while reducing cryptographic choke points as far as possible. Compatibility is not just about protocol semantics; it is also about governance continuity, a critical aspect in ecosystems with several chains sharing infrastructure and decision processes.

Primitive-level strengthening that compromises the sustainability of the ecosystem does not meet this objective.

Table 9 summarizes the four system-level objectives (O1–O4) listed above and links each objective with its most dominant risk driver, its targeted migration mechanism and its associated system-level success condition.

Table 9. System-level objectives under post-quantum constraints.

Objectives (Oi)	Primary Risk Driver	Target Migration Mechanism	System-Level Success Condition
Durability	Temporal exposure (HN DL)	Standardized PQC + legacy lifecycle management	Explicit cryptographic state transition policy
Performance Containment	Validation and propagation overhead	Structural mitigation integrated in consensus design	Validator workload symmetry
Inclusiveness	Resource asymmetry under PQ verification	Hardware-feasible participation	Participation diversity
Compatibility	Cross-chain and governance coupling	Quantum-safe interoperability and governance continuity	Absence of concentrated trust dependencies

These criteria describe constraint dimensions that are used for comparative analysis, not quantitative thresholds for migration strategies to evaluate based on system context and deployment.

The four goals outlined above are not mutually exclusive design goals but rather interacting constraints that restrict a bounded feasibility region for post-quantum migration. Stronger cryptographic security increases the size of the signature and the cost of verification [38]; aggressive performance containment can lead to problems with aggregation and/or externalization, which impact inclusiveness and/or the distribution of trust [97]; tight inclusiveness requirements can cause a decrease in parameter selection and/or verification

time [86], and interoperability hardening can lead to increased latency and/or governance complexity [94].

Migration must be considered as a constrained optimization problem over the multidimensional trade-off surface instead of a series of independent upgrades as suggested by [61]. Migration pathways that are feasible will be those that are within acceptable limits for both durability and performance containment, as well as validator symmetry and ecosystem compatibility.

5.2. Cryptographic Component Selection Under Deployment Constraints

While benchmark comparisons can be used for primitive selection, they should be kept in perspective with respect to the overall maturity, integration feasibility, and architectural alignment of the primitive [98]. Heterogeneity and consensus coordination are typically more challenging to address in blockchain systems than just the cryptographic performance itself.

5.2.1. Lattice-Based Signatures as Baseline Authentication

The method proposed for baseline authentication is lattice-based signatures. After the NIST standardization process, module-lattice constructions (like ML-DSA) are the most deployment-ready authentication primitives [71,81,99]. Comparative analyses in blockchain contexts confirm their feasibility as well as significant size and verification overhead [100]. Their practical suitability is based on the maturity of the ecosystems as well as the depth of formal evaluation and not on the novelty of the theory.

The size of the reported implementations ranges from about 2–3 kB for ML-DSA parameter sets to 64–72 bytes for ECDSA, and the verification costs are about $2 \times$ – $5 \times$ higher depending on the hardware profile and aggregation strategy. This inflation has a direct impact on the size of the transaction payload and the throughput of the validators' tasks in block-constrained environments [9].

Past studies of permissionless blockchains have shown that transaction throughput is ultimately constrained by network propagation delay, block interval, and block size [16].

Assuming fixed block size and a fixed interval, the number of transactions per block is roughly proportional to the ratio of block capacity to average transaction size:

$$\text{Transactions per block} \approx \frac{B}{TxSize_{avg}}, \quad (1)$$

where B is the block size (in bytes) and $TxSize_{avg}$ is the average transaction size (in bytes).

Under otherwise equal protocol parameters, throughput generally decreases as the signature payload comes to dominate the transaction size. Figure 3 illustrates this dependence over the signature size range spanned by classical, lattice-based, and hash-based primitives, using a simplified decomposition $TxSize_{avg} = \beta \times T_{overhead} + S$, where β represents the block configuration and network scaling factor, $T_{overhead}$ denotes the non-signature transaction overhead (inputs, outputs, scripts, and metadata), and S denotes the signature payload size. The sizing parameters underlying the anchor points are compiled from the empirical evaluation data [7,53].

Therefore, a first-order approximation of relative degradation of throughput under post-quantum substitution is given by

$$\frac{TPS_{PQC}}{TPS_{classical}} \approx \frac{S_{classical}}{S_{PQC}}, \quad (2)$$

where TPS_{PQC} and $TPS_{classical}$ represent the transaction throughput under post-quantum and classical systems, respectively, while $S_{classical}$ and S_{PQC} denote their respective average signature sizes in bytes, with all other transaction fields held constant.

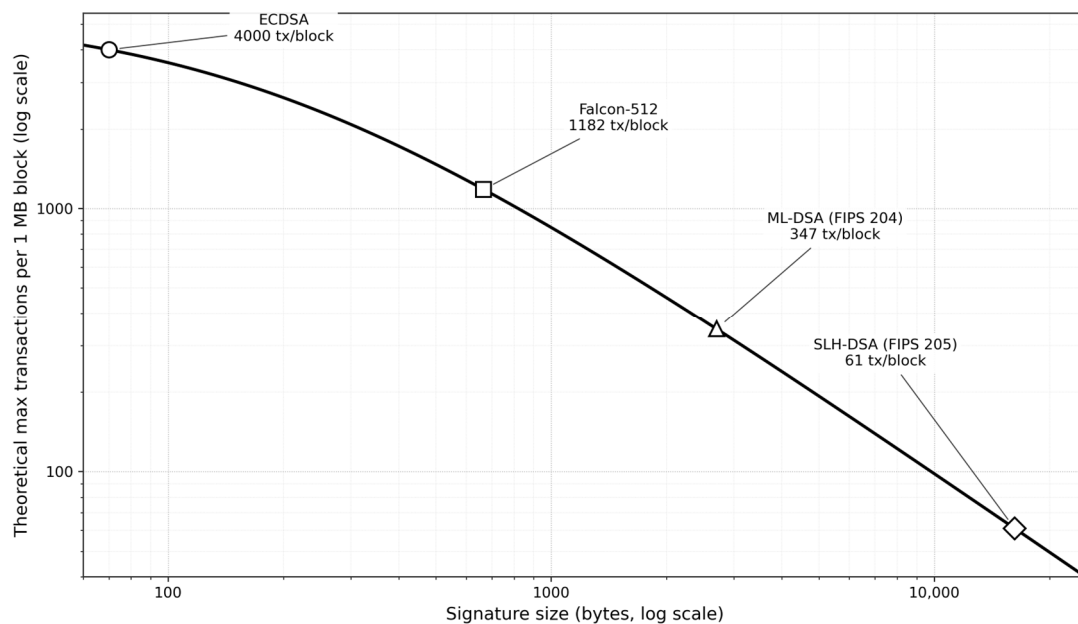


Figure 3. Block-capacity-bound throughput as a function of signature size under a fixed 1 MB block size regime, based on the evaluation model in Equation (1). Anchor points correspond to NIST-standardized primitives (FIPS 203/204/205) and Falcon-512 as a compact lattice alternative.

In practice, while block size and interval are maintained the same, the combined impact of a $3\times$ increase in verification cost and a proportionate increase in block size due to signature inflation may restrict throughput. This shows that there is not an additive but rather a multiplicative relation between the byte inflation (C1) and verification cost amplification (C2) in block-constrained systems.

The relation is a capacity-bound and not a deployment-level performance prediction. It assumes that block size is constant, block interval is constant, there are no aggregation mechanisms, and it validates with full nodes.

This simplified calibration aligns with prototype-level observations, where, under fixed-capacity regimes, the transaction density is significantly affected when replacing classical signatures of ~ 70 bytes with signatures of kilobytes in scale, which are post-quantum [71].

To use a simplified numerical example to demonstrate that such a structure is bound, consider a permissionless blockchain with a fixed block capacity. Suppose that the maximum block size is 1 MB ($\approx 1,000,000$ bytes) and that the average size of a classical transaction is about 250 bytes, including a 70-byte ECDSA signature. As per these assumptions, the theoretical cap on transactions per block is around $1,000,000/250 \approx 4000$ transactions per block:

$$1,000,000/250 \approx 4000 \text{ transactions per block.}$$

The average transaction size, with the classical signature replaced by a ~ 3000 -byte signature based on lattices (while keeping all other transaction fields unchanged) is roughly

$$250 - 70 + 3000 \approx 3180 \text{ bytes.}$$

The block rate (theoretical) is thus

$$1,000,000/3180 \approx 314 \text{ transactions per block.}$$

While this is a simplified, capacity-bound diagram and not a benchmark for a particular deployment, it illustrates that, without any aggregation, compression, or structural mitigation mechanisms, naïve primitive substitution under a fixed set of protocol parameters can lead to a more than tenfold decrease in theoretical transaction density [3].

For reference, Table 7 shows a capacity estimation based on a scenario assumption with a fixed block size of 1 MB for the structural throughput bound calculated above. This is not intended to give a set of deployment-level benchmarks, but rather to show examples of first-order transaction density constraints where the signature size reported by a standardized or prototype implementation is used in place of some other signature size in otherwise unchanged transaction structures. The estimates do not include aggregating, batching, compression, or protocol-level redesign mechanisms [30].

As shown in Table 10, with fixed-block-capacity assumptions, transaction density decreases with signature payload expansion, without the use of structural mitigation mechanisms. The comparison is not about the actual live-network throughput, but it does show the extent of first-order capacity pressure caused by signature substitution in the post-quantum world.

Table 10. Scenario-based estimation of transaction density under representative signature integration (fixed 1 MB block assumption).

Scenario	Approx. Signature Size (Bytes)	Estimated Avg. Tx Size (Bytes) *	Theoretical Max Tx per 1 MB Block	Relative Density vs. Classical Baseline	Dominant Stress Channel
Classical ECDSA baseline	~70	~250	~4000	1× (reference)	—
ML-DSA (module-lattice, FIPS 204 class)	~2700	~3180	~314	~0.08×	C1 + C2
Falcon (compact-lattice-based)	~1200	~1380	~724	~0.18×	C1 dominant
SLH-DSA (hash-based, conservative parameters)	~8000–16,000	~8180–16,180	~61–122	~0.02–0.03×	C1 strongly dominant
Hybrid (ECDSA + ML-DSA)	~2770	~2950	~339	~0.08–0.09×	C1 + C2

* Estimated average transaction size combines the per-scheme signature size with a representative non-signature transaction payload (inputs, out-puts, and metadata); reported values are indicative estimates for cross-scheme comparison rather than exact byte counts. Structural comparison assumes a baseline classical transaction size of ~250 bytes (with ~70 bytes signature part). Non-signature transaction parts are assumed to be constant. Estimates are first-order capacity bounds and should not include any aggregation, batching, compression, or protocol-level optimizations.

These are structural capacity bounds estimates that are made under simplified assumptions and should not be regarded as benchmarks for deployment [43]. They do not include changes to the validator workload, mempool dynamics, feedback effects in the fee market, nor adaptive protocol redesign [99]. Therefore, the results of the analysis should be treated as first-order architectural stress calibration and not as an empirical performance evaluation.

Importantly, the degradation of effective throughput can result from more than just density contraction, as can be achieved through verification cost amplification (C2) in parallel with byte inflation (C1) when the validators are constrained in terms of processing power. These results underline the need for structural mitigation strategies, like aggregation, batching, or layered execution, instead of direct primitive substitution [101].

Though its signature size does not necessarily reflect all of the data for a transaction, in block-constrained systems, such inflation causes measurable pressure on transaction density and propagation dynamics. Experimental tests for quantum-resistant blockchain prototypes show significant slow-downs in throughput in such scenarios [40].

Lattice-based signatures are used in blockchain architectures for transaction authorization, validator identity verification, and governance voting, but structural changes in block formats, validation pipelines, and storage semantics are needed for integration [11]. Transaction-size expansion in a lattice-based authentication can result in block size inflation factors in naïve substitution cases ranging from $10\times$ to $30\times$. Empirical results with the NTRU-based blockchain architecture show that performance containment can be realized only if signature handling and aggregation logic is built into the architecture itself and not added on as an afterthought [102].

Lattice-based signatures are, therefore, quantum-resistant signature primitives as long as architectural containment is built in from the outset.

5.2.2. Hash-Based Signatures for High-Assurance Control Paths

SLH-DSA is a conservative security based mainly on hash-based assumptions [82,103]. However, size and state concerns make it impractical to integrate such constructions at high frequency throughout all transactions, but it is structurally defensible to consider integrating selectively into low frequency in high-assurance control paths. For high-frequency transaction layers, signatures of size larger than 8 kB may be produced by stateless hash-based schemes such as SLH-DSA, which would make them unsuitable, but they would be suitable for infrequent control-plane artifacts [101].

The quantum risk assessment identifies control-plane vulnerabilities, especially those relating to code signing and identity certification, as priority exposure domains [104]. Hash-based signatures thus strengthen the authorization of treasuries [38], the validation of the protocol upgrade, and high-value governance artifacts without creating an overhead at the system level [61].

Layered security with selective deployment decouples control-plane durability from transactional throughput constraints.

5.2.3. Post-Quantum Key Encapsulation for Network Channels

Classical key exchange is a topic of discussion within TLS-layer security as well as inter-node communication, although the former is usually the focus. Migration to quantum-resistant key encapsulation mechanisms like ML-KEM is thus becoming more important now [31,72,80].

The handshake and latency overhead of PQ-integrated TLS in resource-constrained environments has been shown to be non-trivial [105]. In a hybrid ML-KEM deployment, empirical measurements show handshake sizes grow by about $3\times$ – $6\times$ and the latency overhead ranges from 10 to 40% for various network topologies and validator hardware differences. As a result, in heterogeneous validator networks, such overhead can have an indirect impact on propagation times and the connectivity of validators [40], and integration should be synchronized to protocol-layer performance containment and not be considered as a standalone network upgrade [59].

5.2.4. Hybrid and Crypto-Agile Deployment

In decentralized systems with disparate upgrade cycles, full and immediate primitive replacement is impractical [34]. Hybrid cryptographic models are those where classical and post-quantum primitives will coexist during the transition period, enabling operational continuity until at least one primitive is not compromised [89].

Semantic alignments are normally added to classical authentication to create a hybrid transaction format, which could cause the transaction to be temporarily larger, up to a factor of two or three, in migration windows [50,58].

But the extensibility of transactions by a dynamically selected format is an essential part of hybrid windows [106] and so is the need to validate transactions using multiple

primitives as well as the governance-controlled mechanisms of activation and deprecation [51]. Agility, as a structural requirement, not flexibility, is consistently the focus of surveys related to the transition to post-quantum blockchain [69]. Hybrid coexistence is thus viewed more as a state of transition than as an equilibrium.

5.3. Performance Containment and Mitigation Architecture

Signature inflation and verification complexity passes through the validation and propagation layers, so mitigation must be done structurally, not reactively [9].

Most architectural mitigation strategies fall into one of two categories: aggregation-based and fault-isolation-based, with the former being ways of reducing the signature payload while sacrificing the extent of fault isolation [107,108]. Temporal batching amortizes verification cost but introduces latency considerations.

Tiered authentication provides a balance between the level of security needed for each transaction and the level of governance that is required. Optimization of payload and deterministic encoding can minimize propagation pressure without affecting cryptographic complexity [109]. Strong penalty mechanisms lead to a smooth workload of the validators when a verification is deferred or staged [66]. Layer-2 or off-chain execution shifts high-frequency PQ workloads off-chain, with the potential of adding further assumptions of trust or dispute resolution [15].

It is necessary to evaluate not only the performance improvements of mitigation mechanisms but also their impact on validator symmetry and validator trust concentration. Interoperability surveys warn that some optimization that is done by a committee can create new centralized choke points if not bound correctly [110].

Instead of relying on purely qualitative reasoning, the structural throughput bound under fixed-block-capacity assumptions can be formalized using results from the previous performance modeling:

$$TPS \approx \frac{B}{\bar{T}} \times \frac{1}{V}, \quad (3)$$

where B is the block size in bytes, $\bar{T}$ is the average transaction size in bytes, and V is the relative per-transaction verification cost factor against the classical baseline [4,10,68]. Equation (3) gives a capacity-normalized throughput proxy (transactions per block, rescaled by the relative validation cost).

For a simplified calibration, assume a fixed-capacity blockchain, where $B = 1$ MB and an average transaction size $\bar{T} = 3180$ bytes, with the post-quantum substitution model, as shown above. With a conservative scaling factor of $V \approx 3$, the effective scaling factor for throughput is roughly $1/V \approx 1/3$.

The compound effect suggests that in addition to byte inflation, validator-side processing constraints lead to throughput pressure. From a practical standpoint, if the block size does not change, then a bigger verification latency can lead to a lower effective throughput or can result in more stringent hardware assumptions to maintain the block interval [34].

The example is simplified and does not make predictions about the performance at deployment, but it shows that capacity $B/TxSize_{avg}$ and verification cost V are coupled in post-quantum integration scenarios.

Here are some structural constraints that make mitigation strategies like aggregation, compression, or Layer-2 migration unavoidable [105,111].

5.4. Interoperability Under Asymmetric Migration

Blockchain connectivity includes connectors, relays, light clients, and hybrid frameworks [68]. In quantum threat models, the cryptographic trust concentration in the bridge committees or threshold relays becomes an amplification vector [30].

Furthermore, there are security mismatches due to the different migration timelines by chain. Some systems may use PQ primitives sooner rather than later, and others may continue to use classical assumptions for longer periods of time. The interoperability layers need to be able to ignore and live with heterogeneous cryptographic baselines and not make any assumptions about the timing of the upgrades [64].

Light-client verification involves only less explicit trust, but there are an increased bandwidth and proof-size overhead when using PQ signatures [92]. To avoid cross-chain cascading effects, structural bounds on the complexity of verifying a statement become necessary, as do explicit containment domains.

Interoperability becomes a constraint of migration, not an afterthought design consideration.

5.5. Governance as a Migration Constraint

In Section 4, governance fragility was examined in relation to quantum threat exposure. In this case, governance is considered one of the constraints of migration.

First, governance latency directly affects the length of time over which exposure occurs. To enable decentralized coordination, there needs to be proposal drafting, deliberation, client implementation, and network-wide adoption. In a time-asymmetric threat model, a quantum-vulnerable artifact may remain active throughout this deliberation period [112].

Second, legacy cryptographic persistence makes for historical finality. Historical signatures are still valid as per the consensus rules, even when using PQ primitives for new transactions. Governance, therefore, needs to establish policies for revalidation, acceptable residual risk, and archival treatment for artifacts that are vulnerable to quantum threats [113].

Third, incentives for adoption affect the ability to make upgrades. Regulatory cost and coordination barriers are noted to be ongoing challenges in the blockchain adoption process through systematic reviews [114]. The technical effectiveness of migration strategies can become frustrated without incentive alignment.

Last, if participation is made more restrictive by hardware, governance capture risk may be exacerbated by the increased demand for resources [94]. Thus, migration pacing should be coordinated with the capacity of the validators and the coordination of the ecosystem.

Governance capacity drives a possible pathway for the quantum–post-quantum transition.

5.6. Integrated Migration Roadmap

The previous sections make it clear that post-quantum migration is not a basic substitution problem but a constrained system reconfiguration problem. Section 4 has shown how quantum stress cascades down the cryptographic, protocol, network, interoperability, and governance layers. Section 5 mapped those stress channels to design objectives and constraints for mitigation. What remains is the question of when those constraints occur at the same time and how migration progress becomes formalized.

There is not necessarily a main migration route. The cost of validation structures is changed by cryptographic upgrades [16]. Cost shifts in validation affect the propagation and construction of blocks [65]. The propagation changes convert consensus security margins [108], while the interoperability constraints create cross-domain exposure [94]. Hybrid states may last for a certain period, depending on governance pacing [106]. The coupled system of these interactions can be overlooked if the roadmap processes the layers one at a time instead of modeling them; otherwise, it is possible to widen the instability in the system instead of eliminating it [61].

Thus, the roadmap is presented as a step-by-step sequence of layer-by-layer developments over a bounded trade-off surface, not as a list of technology replacements.

5.6.1. Cross-Layer Dependency Structure

Post-quantum migration operates over four tightly coupled domains:

- The cryptographic layer—signature schemes, key encapsulation, and identity primitives;
- The protocol and execution layer—transaction formats, validation logic, and block structure;
- The network and interoperability layer—propagation, cross-chain verification, and bridge trust assumptions;
- The governance layer—upgrade coordination, enforcement asymmetry, and validator participation incentives.

Any changes in one domain automatically affect the other domains' feasible operating conditions. For instance, enlarged signatures will have higher payloads per block and verification costs. Validator resource cost is no longer symmetric due to increased verification costs [115]. The more asymmetric the validator, the more likely the risk of capture is by governance [6]. There is a loss of interoperability security assumptions due to the hybrid enforcement windows, which create a longer exposure period.

This dependency is such that migration needs to maintain constraint equilibrium between domains at every stage [43]. An upgrade that is not within the validator's resource limit is a violation of O3. Long delays in the governance process lead to the continuation of hybrid cryptography, which is a violation of O1. A protocol redesign that requires a reduction in throughput is not considered O4.

Migration, as defined in the roadmap, is thus a system trajectory that traverses the surface of trade-offs in Section 5.1 without crossing the boundaries of destabilizing constraints. A small-scale migration route, with a limited range of movement as outlined above, is represented in Figure 4.

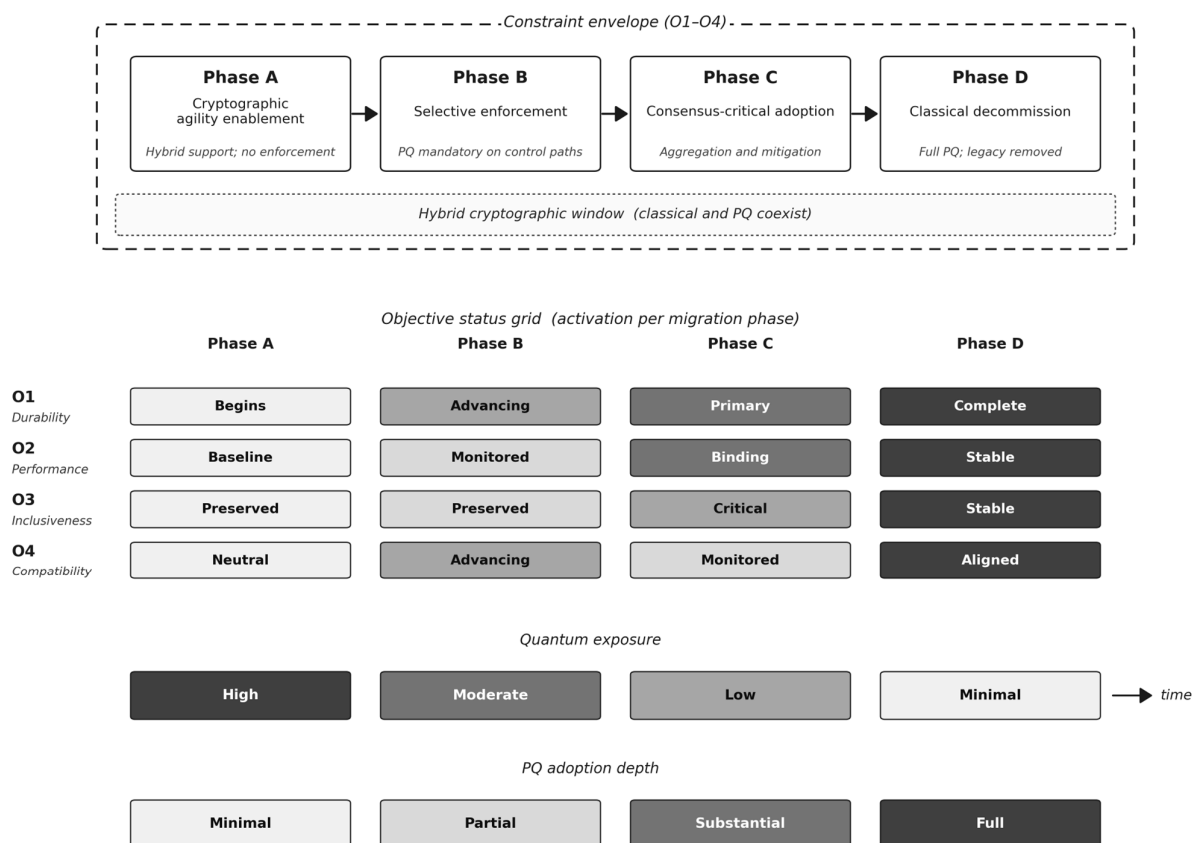


Figure 4. Phase-based post-quantum migration trajectory within the constraint envelope defined by O1–O4.

5.6.2. Capability-Based Phased Transition

This is because of two factors:

- Threat maturity is not known;
- Migration is organized on capacity states, not calendar deadlines.

Governance latency is endogenous to blockchain systems. Each phase increases the possible region of operation in the post-quantum world [116].

Phase A—Cryptographic Agility Enablement

During this phase, multi-primitive support will be available by using hybrid verification logic (non-enforcement). The primary objective of this phase is to provide visibility to the object and not replace it [11].

The key features of Phase A are the following:

- Support for standardized post-quantum signatures and key encapsulation mechanisms [117];
- Explicit tagging of cryptographic provenance in transactions;
- Measurement of the performance deltas that occur when validators are actively validating [115].

The design space is optimized during this phase while ensuring operation stability. The main concern during this phase is providing extra support for O1 (durability) while maintaining O2 (performance containment) and O3 (validator inclusiveness).

Phase B—Selective Enforcement on Control Paths

Examples of post-quantum primitives needed for high-assurance control-plane operations, treasury governance, validator identity, and cross-chain bridge authentication. Hybrid models are still used for high-frequency transactional paths to avoid sudden throughput failures. Empirical research on post-quantum blockchain architecture shows that one can maintain overheads that are within acceptable bounds if used in a constrained setting when selectively enforced [118].

This phase minimizes system exposure yet does not lead to workload instability when it comes to transactions. O1 is then promoted, O4 is promoted, and attempts are made to prevent too much decentralization of O2.

Phase C—Consensus-Critical Post-Quantum Adoption

The primitives that are part of consensus are also extended to the post-quantum. Legacy validation contexts are the only ones that support classical schemes. These mechanisms are all combined: aggregation, batching, tiered authentication, and off-chain amortization [106].

This is when the workload symmetry of the validator becomes a major constraint, interoperability mechanisms must be re-evaluated, and the governance capture risk must be monitored in the case of increased resource demands [97]. Today the system runs on a basis of post-quantum assumptions, and still there is cryptographic material that is not based on the post-quantum assumption.

Phase D—Classical Primitive Decommissioning

Removal of quantum-unsafe primitives happens only once ecosystem coordination thresholds are met, cross-chain partners are at compatible security baselines, and validator participation remains stable [14].

Avoid premature decommissioning, or the risk of ecosystem fragmentation, by extending exposure windows. This phase therefore depends on governance, not on technology, in terms of cryptographic finality. Without realizing appropriate full alignment (O1–O4), the classical primitives should not be decommissioned to avoid ecosystem compatibility destabilization.

5.6.3. Hybrid Window Management

One of the most unique characteristics of post-quantum migration is that of the hybrid window, the time window that starts when classical and post-quantum cryptography exist side by side [51]. This window introduces three structural tensions:

- Exposure persistence under harvest-now–decrypt-later dynamics;
- Verification asymmetry between validators;
- Governance enforcement inconsistency.

Explicit bounds for classical acceptance policies for legacy signatures, defined revalidation/re-signing policies, and rate-limited enforcement escalation are required for the hybrid window. It is not about being “pure” overnight; rather, it is about decaying exposure in a controlled manner.

5.6.4. Interoperability Alignment Under Asymmetric Adoption

Blockchains do not move around alone. Trust models and bridge architectures are also found to be different across the various interoperability mechanisms, as shown in empirical surveys of the mechanisms [11]. If the migration timing is asymmetric, then exposure of strong chains will be passed to their weaker bridge endpoints, and proof sizes will be inflated in committee-based connectors under post-quantum verification [3,6].

The roadmap, therefore, incorporates containment principles:

- Domain separation between bridge and consensus keys;
- Explicit cryptographic baseline disclosure;
- Isolation mechanisms for lagging systems.

Interoperability is treated as a migration multiplier rather than a peripheral feature.

5.6.5. Governance-Constrained Adaptation

Governance affects the speed of migration. Empirical adoption studies further validate the cost, regulatory uncertainty, and technical understanding impacts on upgrade willingness [119].

The roadmap includes feedback loops, monitoring validator participation changes, measuring performance loss under enforced PQ workloads, and recalibrating the scope of enforcement when decentralization is at risk. Migration is adaptive, but system-level objectives bound adaptation.

5.7. Synthesis

Post-quantum migration in blockchain systems is an optimization architectural problem with constraints on durability, performance containment, inclusiveness, and compatibility [103]. Resilience is not just achieved through primitive substitution. Security is a result of balance in cryptographic assurance, validator symmetry, interoperability alignment, and governance capacity.

Approaches that rely on isolated cryptographic strength but neglect these coupled constraints can be expected to merely redistribute, rather than lessen, fragility systemically.

6. Open Research Challenges and Future Directions

The roadmap mentioned in Section 5 should be understood as a working migration framework and not as a set plan for implementation. It captures the practical limitations that have already been observed in ongoing post-quantum migration efforts and affords the possibility of empirical corrections as evidence of deployment grows [120]. Rather, its aim is to organize those questions that the literature so far treats only fragmentarily and not to determine the “winner algorithm”.

It is worth noting that there are some issues not yet resolved that cannot be solved by replacing primitives or by redesigning a single protocol entity. Decentralization limits, coordination delay, and the longevity of long-lived validation decisions are the most difficult issues with system behavior [121]. The reason for these issues is that, when post-quantum assumptions are considered, security, performance, and governance do not run independent of one another. Therefore, this section focuses on some research gaps that are frequently mentioned in the literature but are only partially realized as system-level models.

6.1. Measuring Post-Quantum Trade-Offs

It is difficult to quantify post-quantum trade-offs [72]. In recent research, performance metrics are typically reported separately, security enhancements are still expressed at the algorithm or primitive level, and participation and decentralization effects are omitted and not fully measured [29].

A practical way forward is to consider post-quantum overhead as a quantifiable propagation and participation problem, rather than as a single number [58]. Even a minimal, shared indicator set would aid in structuring analysis on other bytes per transaction, cost of signature verification, and propagation delay between heterogeneous validators [16].

Also, these metrics need to be compared by their effects of on validator participation and effective decentralization, not just against throughput [35]. Such measurements would render O2 (performance containment) and O3 (validator inclusiveness) as empirically testable constraints, instead of abstract design targets.

Even the most basic sensitivity test (such as an increase in retention versus verification latency) would move away from the “overhead exists” discussion to a more decision-relevant one: how much overhead affects who can still participate in high-stakes application settings, where participation may already be fragile? [86].

6.2. Cryptographic Agility Under Uncertain Quantum Timelines

Uncertainty surrounding quantum capabilities considerably complicates protocol planning [30]. Historical stability is a key component of trust substrates in general, which tends to make disruptive upgrades difficult on blockchains, but it is not so convenient when the security lifetime of deployed primitives is not expressed in a clean manner [122].

One direction of relevance in this research is modeling the transition from the classical world to the quantum world as a stepwise process instead of a transition event. The measurable variables—upgrade latency, coordination overhead, and validator cost temporal asymmetry—can be used to assess each stage of the discrete upgrade stages: hybrid coexistence, partial validator adoption, and delayed validator activation [10,121].

Furthermore, a hypothesis based on a scientific timeline should be evaluated based on likely quantum progress signals [113]. Although not predictive in any way, even simplified comparative simulations can provide insight into the role that scheduling strategies can play in promoting governance responsiveness, validator participation, and protocol stability in the presence of delayed-risk scenarios [123]. This way, the discussion remains focused on the consequences of scheduling decisions and not on the dates.

6.3. Legacy Cryptographic Exposure and Historical Validity

One aspect which is still not explored is the treatment of historical data that has been authenticated by quantum-vulnerable primitives [72]. Immediately after the full shift of post-quantum cryptography to new transactions, legacy transactions continue to be stored and are still “operationally valid” according to the old rules [12] (as are smart contracts and governance decisions).

There are two open research issues here: technical (revalidation, re-signing, archival semantics) and institutional. The level of acceptable residual risk for long-lived assets and

the circumstances under which a chain is justified in modifying historical authenticity is not clearly defined [124]. The literature in this field remains narrow, and deployment-level proposals for dealing with exposure remain underdeveloped compared to forward-looking statements of cryptographic substitution, which is why legacy exposure is an immediate extension of O1 (durability) beyond just forward-looking cryptographic substitution.

6.4. *Post-Quantum Interoperability at the Ecosystem Level*

Migration can significantly add to post-quantum risk as it is an asynchronous operation between chains, and bridge mechanisms can focus verification and trust responsibility [97]. In the literature, the repeated trend is to study interoperability as a stand-alone mechanism and not as a component of an “ecosystem” of interconnected chains and shared infrastructure [125].

A chain could similarly achieve a local post-quantum resilience but also be exposed via composability, relays, and cross-domain authentication [37]. This is especially important in network-based blockchain implementations and IoT-type environments, where endpoints are diverse and periodic upgrades are irregular [126].

Future research should therefore consider interoperability as a multiplier of migration: identifying the cross-chain edges on which the two are exposed and then experimenting with containment strategies, including domain separation of keys, baseline disclosure, and isolation of lagging endpoints under realistic message and trust models.

6.5. *Governance Dynamics as a Limiting Security Constraint*

Governance is not a neutral coordination wrapper in post-quantum migration, but rather it is a constraint on security. Conditions of uncertainty, split incentives, and differing participation in which decentralized communities must deal with technically complex and economically disruptive proposals are precisely the conditions where coordination failure becomes security-relevant rather than just “slow” [37]. Within this context, governance performance acts as a constraint on the possible migration region, not as a background coordination variable.

Governance behavior in the post-quantum era is still poorly understood empirically. There is limited evidence on the governance response to delayed threat realization, cryptographic uncertainty, and asymmetric exposure; as a result, the existing theoretical governance models account for only part of the actual outcomes of governance that are observed in large ecosystems [87].

A practical approach is to institute governance practice through codes of observable governance responses that go beyond the success/failure label [127]. Researchers can monitor the time to activation, the validator participation dynamics during the process of the contentious upgrade, quorum instability and enforcement asymmetry and then compare their observations to structured post-quantum upgrade scenarios [18].

In addition, in the context of ideas for quantum-native authentication and quantum signature, they should be assessed not only for security novelty but also for the feasibility of governance and deployment burden; otherwise, they are “interesting but non-migratable” [128].

In all these challenges, the common thread is that the issues are not independent of each other, but rather interconnected. The various layers of quantification, agility, legacy exposure, interoperability, and governance constraints interact over time and over layers. Such considerations [16,88] will not be enough to focus only on cryptographic substitution. What is missing is a modeling of the technical, economic, and coordination aspects at the system level, integrated into a single framework expressible in terms of evaluation [129].

7. Limitations

There are several limitations to this review. The first is that the literature retrieved is restricted to English-language peer-reviewed research, which could exclude relevant regionally conducted research, and the second is that the rapidly changing nature of PQC standardization and implementation may make it more difficult to find some of the latest results in peer-reviewed literature. Third, the metrics and measures used across studies are not consistent across platforms and baselines, thus making formal meta-analysis a less important part of the review and leaving a focus on qualitative synthesis and dependency mapping. Last, contribution-based synthesis adds depth to the analysis but can under-represent broadly applicable empirical findings that are only narrowly scoped. Finally, title and abstract screening was performed by a single screener using a predefined relevance-scoring protocol rather than by two independent reviewers; accordingly, a formal inter-rater agreement statistic (e.g., Cohen's κ) was neither pre-registered nor computed. This subjectivity was mitigated through explicit, reproducible eligibility criteria, although fully independent dual screening would further strengthen the robustness of study selection.

8. Conclusions

Migration from a classical to post-quantum world in a blockchain cannot be simplified as a cryptographic replacement. While signature schemes and key encapsulation mechanisms are the most obvious elements to consider in the transition, the dimensions of analysis presented in this review are analytically distinct but operationally connected in the architectures of live blockchains.

While it is clear that the transition from classical to post-quantum alternatives does not equate to system-level resilience, it is important to remember that the challenge of establishing a resilient system lies in more than just those options. Second-order impacts on validator participation, hardware symmetry, economic feasibility, and governance responsiveness include signature expansion, increased verification cost, and changed propagation timing. These changes could over time be clearly recognized to affect decentralization thresholds even if the formal improvement in cryptographic strength is not manifested [30,62].

This review provides a framework that is system-level in nature and combines five architectural stress channels (C1–C5) and four bounded migration objectives: cryptographic durability, performance containment, validator inclusiveness, and interoperability–governance compatibility. The framework does not outline one implementation trajectory but rather an understanding of how migration decisions will rebalance constraints in a way that is embedded in multiple interdependent layers of technology and institutions.

The main structural results are the following:

1. The post-quantum transition is not simply a primitive replacement but a stress propagation between layers and thus must be addressed through coordinated architectural adaptation;
2. Under fixed block capacity and fixed timing constraints, signature inflation (C1) and verification amplification (C2) are coupled, thus reducing the performance range;
3. Governance latency and hybrid cryptographic windows are multiplicative factors of temporal exposure under harvest-now–decrypt-later dynamics;
4. Asymmetric migration risk increases because of layers of interoperability and cross-chain mechanisms if timelines for adoption differ between ecosystems;
5. Sustainable migration is about reaching a bounded equilibrium between durability, performance containment, validator symmetry, and ecosystem compatibility, not just cryptographic strength.

The operational implications of these findings suggest that the move to post-quantum readiness should not be viewed as a cryptographic patch but as a staged architectural

transition that will require action by the blockchain infrastructure operator—be it a validator network, bridge operator, or consortium administrator.

Also, post-quantum compatibility is likely to be part of security certification standards set by the standardization bodies and industry consortia and be part of long-term digital asset governance structures. To avoid security-driven participation concentration, governance processes should, therefore, incorporate explicit upgrade pacing, hybrid-window management, and validator-capacity monitoring.

A coordinated standardization, protocol engineering, and regulatory policy alignment will thus be critical to ensure that quantum resilience does not weaken but strengthens decentralized ecosystems. Despite these contributions, the following limitations must be recognized: the present work is a structural analysis and synthesis rather than deployment benchmarking of the analysis results across heterogeneous live environments.

Empirical validation across real validator workloads, cross-chain infrastructures, and staggered governance responses is still limited. Further research should also focus on measurable trade-off modeling, assessment of interoperability at the ecosystem level, and analysis of governance behavior for asymmetric upgrades.

In the end, post-quantum security is the outcome of a coordinated adaptation of the cryptographic, infrastructure, and governance levels to respond to changing threat models and is not the strength of a single primitive.

Supplementary Materials: The following supporting information can be downloaded at <https://www.mdpi.com/article/10.3390/technologies14060367/s1>, Table S1: Screening register of all identified records ($n = 234$).

Author Contributions: Conceptualization, F.S.S., E.I. and S.P.; methodology, F.S.S., E.I. and S.P.; software, F.S.S., E.I. and A.P.; validation, F.S.S., E.I., S.P., A.P. and A.N.; formal analysis, F.S.S., E.I., S.P. and A.N.; investigation, F.S.S., E.I., S.P., A.P. and A.N.; resources, S.P.; data curation, F.S.S., E.I., S.P., A.P. and A.N.; writing—original draft preparation, F.S.S., and E.I.; writing—review and editing, F.S.S., E.I., S.P., A.P. and A.N.; visualization, F.S.S., E.I. and A.P.; supervision, E.I.; project administration, S.P.; funding acquisition, S.P. All authors have read and agreed to the published version of the manuscript.

Funding: The results were obtained with the financial support of the project “Technologies for countering previously unknown quantum cyber threats”, implemented within the framework of the state program of the “Sirius” Federal Territory “Scientific and technological development of the “Sirius” Federal Territory” (Agreement No. 23-03 dated 27 September 2024). The APC was funded by the state program of the “Sirius” Federal Territory “Scientific and technological development of the “Sirius” Federal Territory” (Agreement No. 23-03 dated 27 September 2024).

Data Availability Statement: Data is contained within the article and the Supplementary Materials (Table S1).

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

C1–C5	Architectural Stress Channels
O1	Cryptographic Durability
O2	Performance Containment
O3	Validator Inclusiveness
O4	Interoperability–Governance Compatibility
DAO	Decentralized Autonomous Organization
ECDSA	Elliptic-Curve Digital Signature Algorithm
HNDL	Harvest Now, Decrypt Later
KEM	Key Encapsulation Mechanism

ML-DSA	Module-Lattice-Based Digital Signature Algorithm
ML-KEM	Module-Lattice-Based Key Encapsulation Mechanism
NIST	National Institute of Standards and Technology
PQC	Post-Quantum Cryptography
PETs	Privacy-Enhancing Technologies
PoS	Proof-of-Stake
PoW	Proof-of-Work
RSA	Rivest-Shamir-Adleman
SHA-256	Secure Hash Algorithm 256-Bit
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm
TLS	Transport Layer Security
TPS	Transactions Per Second
ZKPs	Zero-Knowledge Proofs

References

- Revathi, K.; Suganthi, K. Enhancing Blockchain Security against Quantum Threats through Integration of Post-Quantum Cryptographic Algorithms. *Comput. Electr. Eng.* **2025**, *127*, 110610. [\[CrossRef\]](#)
- Marchsreiter, D. Towards Quantum-safe Blockchain: Exploration of PQC and Public-key Recovery on Embedded Systems. *IET Blockchain* **2025**, *5*, e12094. [\[CrossRef\]](#)
- Abbasi, M.; Cardoso, F.; Váz, P.; Silva, J.; Martins, P. A Practical Performance Benchmark of Post-Quantum Cryptography Across Heterogeneous Computing Environments. *Cryptography* **2025**, *9*, 32. [\[CrossRef\]](#)
- Prajapat, S.; Thakur, G.; Kumar, P.; Das, A.K.; Hossain, M.S. A Blockchain-Assisted Privacy-Preserving Signature Scheme Using Quantum Teleportation for Metaverse Environment in Web 3.0. *Future Gener. Comput. Syst.* **2025**, *164*, 107581. [\[CrossRef\]](#)
- Malina, L.; Dzurenda, P.; Ricci, S.; Hajny, J.; Srivastava, G.; Matulevičius, R.; Affia, A.-A.O.; Laurent, M.; Sultan, N.H.; Tang, Q. Post-Quantum Era Privacy Protection for Intelligent Infrastructures. *IEEE Access* **2021**, *9*, 36038–36077. [\[CrossRef\]](#)
- Chen, T.-H.; Hung, W.-H. Feasibility and Limitations of Generalized Grover Search Algorithm-Based Quantum Asymmetric Cryptography: An Implementation Study on Quantum Hardware. *Electronics* **2025**, *14*, 3821. [\[CrossRef\]](#)
- Javaid, M.A.R.; Ashraf, M.; Rehman, T.; Tariq, N. Impact of Post Quantum Digital Signatures on Block Chain: Comparative Analysis. *Asian Bull. Big Data Manag.* **2024**, *4*, 121–138. [\[CrossRef\]](#)
- Juaristi, P.; Agudo, I.; Rios, R.; Ricci, L. Benchmarking Post-Quantum Cryptography in Ethereum-Based Blockchains. In *Computer Security. ESORICS 2024 International Workshops; Lecture Notes in Computer Science*; Springer: Cham, Switzerland, 2025; Volume 15263, pp. 340–353. [\[CrossRef\]](#)
- Marengo, A.; Pagano, A. Investigating the Factors Influencing the Adoption of Blockchain Technology across Different Countries and Industries: A Systematic Literature Review. *Electronics* **2023**, *12*, 3006. [\[CrossRef\]](#)
- Sinai, N.K.; In, H.P. Performance Evaluation of a Quantum-Resistant Blockchain: A Comparative Study with Secp256k1 and Schnorr. *Quantum Inf. Process.* **2024**, *23*, 99. [\[CrossRef\]](#)
- Yuan, B.; Wu, F.; Zheng, Z. Post Quantum Blockchain Architecture for Internet of Things over NTRU Lattice. *PLoS ONE* **2023**, *18*, e0279429. [\[CrossRef\]](#) [\[PubMed\]](#)
- Marchesi, L.; Marchesi, M.; Tonelli, R. A Survey on Cryptoagility and Agile Practices in the Light of Quantum Resistance. *Inf. Softw. Technol.* **2025**, *178*, 107604. [\[CrossRef\]](#)
- Radanliev, P. Cyber Diplomacy: Defining the Opportunities for Cybersecurity and Risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *J. Cyber Secur. Technol.* **2025**, *9*, 28–78. [\[CrossRef\]](#)
- Neethu, V.A.; Khan, M.A. Securing Data Privacy and Integrity in Cloud Computing Using Blockchain and Quantum Cryptography. *Metall. Mater. Eng.* **2025**, *31*, 137–145. [\[CrossRef\]](#) [\[PubMed\]](#)
- Islam, M.J.; Islam, S.; Hossain, M.; Noor, S.; Islam, S.M.R. Securing Blockchain Systems: A Layer-Oriented Survey of Threats, Vulnerability Taxonomy, and Detection Methods. *Future Internet* **2025**, *17*, 205. [\[CrossRef\]](#)
- Arslan, R.; Özseven, T.; Aydın, M.M. Transforming European Cybersecurity: AI-Powered Threat Analysis, Quantum Age, Blockchain/Crypto Risks, and Regulatory Strategies. *Int. J. Eng. Appl. Sci.* **2025**, *17*, 81–93. [\[CrossRef\]](#)
- Fernández-Caramés, 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. [\[CrossRef\]](#)
- Parida, N.K.; Jatoth, C.; Reddy, V.D.; Hussain, M.M.; Faizi, J. Post-Quantum Distributed Ledger Technology: A Systematic Survey. *Sci. Rep.* **2023**, *13*, 20729. [\[CrossRef\]](#) [\[PubMed\]](#)
- Yang, Z.; Alfauri, H.; Farkiani, B.; Jain, R.; Pietro, R.D.; Erbad, A. A Survey and Comparison of Post-Quantum and Quantum Blockchains. *IEEE Commun. Surv. Tutor.* **2024**, *26*, 967–1002. [\[CrossRef\]](#)

20. Ramzan, M.T.; Cimato, S. Blockchain in the Quantum Era: Surveying Security Challenges and Post-Quantum Cryptography. In Proceedings of the 2025 IEEE 49th Annual Computers, Software, and Applications Conference (COMPSAC), Toronto, ON, Canada, 26 August 2025; pp. 8–11. [\[CrossRef\]](#)
21. Gharavi, H.; Granjal, J.; Monteiro, E. Post-Quantum Blockchain Security for the Internet of Things: Survey and Research Directions. *IEEE Commun. Surv. Tutor.* **2024**, *26*, 1748–1774. [\[CrossRef\]](#)
22. Aggarwal, D.; Brennen, G.K.; Lee, T.; Santha, M.; Tomamichel, M. Quantum Attacks on Bitcoin, and How to Protect Against Them. *Ledger* **2018**, *3*, 68–90. [\[CrossRef\]](#)
23. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *BMJ* **2021**, *372*, n71. [\[CrossRef\]](#) [\[PubMed\]](#)
24. Aounzou, Y.; Boulaalam, A.; Kalloubi, F. Convergence of Blockchain, IoT, and Machine Learning: Exploring Opportunities and Challenges—A Systematic Review. *Int. J. Smart Sens. Intell. Syst.* **2025**, *18*, 20250002. [\[CrossRef\]](#)
25. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; EBSE Technical Report EBSE-2007-01; Keele University: Newcastle, UK; University of Durham: Durham, UK, 2007; Available online: https://legacyfileshare.elsevier.com/promis_misc/525444systematicreviewsguide.pdf (accessed on 28 May 2026).
26. Petersen, K.; Vakkalanka, S.; Kuzniarz, L. Guidelines for Conducting Systematic Mapping Studies in Software Engineering: An Update. *Inf. Softw. Technol.* **2015**, *64*, 1–18. [\[CrossRef\]](#)
27. Akella, G.K.; Wibowo, S.; Grandhi, S.; Mubarak, S. A Systematic Review of Blockchain Technology Adoption Barriers and Enablers for Smart and Sustainable Agriculture. *Big Data Cogn. Comput.* **2023**, *7*, 86. [\[CrossRef\]](#)
28. Saeed, H.; Malik, H.; Bashir, U.; Ahmad, A.; Riaz, S.; Ilyas, M.; Bukhari, W.A.; Khan, M.I.A. Blockchain Technology in Healthcare: A Systematic Review. *PLoS ONE* **2022**, *17*, e0266462. [\[CrossRef\]](#) [\[PubMed\]](#)
29. Samreen, N.F.; Alalfi, M.H. An Empirical Study on the Complexity, Security and Maintainability of Ethereum-Based Decentralized Applications (DApps). *Blockchain Res. Appl.* **2023**, *4*, 100120. [\[CrossRef\]](#)
30. Aslam, A. Quantum Computing Threats to Cryptography: A Comprehensive Analysis of Vulnerabilities, Countermeasures, and Future-Proofing Strategies. *Res. Sq.* **2025**. [\[CrossRef\]](#) [\[PubMed\]](#)
31. Dahhak, H.; Afifi, N.; Hilal, I. Security Analysis of Classical and Post-Quantum Blockchains. *J. Comput. Inf. Syst.* **2024**, 1–14. [\[CrossRef\]](#)
32. Alshahrani, H.; Islam, N.; Syed, D.; Sulaiman, A.; Al Reshan, M.S.; Rajab, K.; Shaikh, A.; Shuja-Uddin, J.; Soomro, A. Sustainability in Blockchain: A Systematic Literature Review on Scalability and Power Consumption Issues. *Energies* **2023**, *16*, 1510. [\[CrossRef\]](#)
33. Zhou, L.; Diro, A.; Saini, A.; Kaisar, S.; Hiep, P.C. Leveraging Zero Knowledge Proofs for Blockchain-Based Identity Sharing: A Survey of Advancements, Challenges and Opportunities. *J. Inf. Secur. Appl.* **2024**, *80*, 103678. [\[CrossRef\]](#)
34. Neethu, V.A. Enhancing Data Privacy and Integrity in Cloud Systems Through Blockchain and Quantum Cryptographic Integration. *J. Inf. Syst. Eng. Manag.* **2025**, *10*, 327–337. [\[CrossRef\]](#)
35. Reno, S.; Roy, K. CrustChain: Resolving the Blockchain Trilemma via Decentralized Storage and Proof-of-Capacity Consensus. *PLoS ONE* **2025**, *20*, e0328395. [\[CrossRef\]](#) [\[PubMed\]](#)
36. Ren, S.; Kim, E.; Lee, C. A Scalable Blockchain-Enabled Federated Learning Architecture for Edge Computing. *PLoS ONE* **2024**, *19*, e0308991. [\[CrossRef\]](#) [\[PubMed\]](#)
37. Aslam, A.M.; Bhardwaj, A.; Chaudhary, R. Quantum-Resilient Blockchain-Enabled Secure Communication Framework for Connected Autonomous Vehicles Using Post-Quantum Cryptography. *Veh. Commun.* **2025**, *52*, 100880. [\[CrossRef\]](#)
38. Chen, J.; Ling, J.; Ning, J.; Panaousis, E.; Loukas, G.; Liang, K.; Chen, J. Post Quantum Proxy Signature Scheme Based on the Multivariate Public Key Cryptographic Signature. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 155014772091477. [\[CrossRef\]](#)
39. Kim, H.; Kim, W.; Kang, Y.; Kim, H.; Seo, H. Post-Quantum Delegated Proof of Luck for Blockchain Consensus Algorithm. *Appl. Sci.* **2024**, *14*, 8394. [\[CrossRef\]](#)
40. Seol, J.; Kim, J. Quantum threat and dependability of quantum-safe blockchainbased distributed control systems and network. *Issues Inf. Syst.* **2023**, *24*, 144–158. [\[CrossRef\]](#)
41. Holcomb, A.; Pereira, G.; Das, B.; Mosca, M. PQFabric: A Permissioned Blockchain Secure from Both Classical and Quantum Attacks. In Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia, 3–6 May 2021; pp. 1–9. [\[CrossRef\]](#)
42. Vermeer, M.J.D.; Heitzenrater, C.; Parker, E.; Moon, A.; Lumpkin, D.; Awan, J. Evaluating Cryptographic Vulnerabilities Created by Quantum Computing in Industrial Control Systems. *J. Crit. Infrastruct. Policy* **2024**, *5*, 88–110. [\[CrossRef\]](#)
43. Hanafi, B.; Ali, M. Analyzing the Research Impact in Post Quantum Cryptography through Scientometric Evaluation. *Discov. Comput.* **2025**, *28*, 32. [\[CrossRef\]](#)
44. Durgut, S.; Küçüksille, E.U.; Tokmak, M. Hybrid Quantum–Classical Deep Neural Networks Based Smart Contract Vulnerability Detection. *Appl. Sci.* **2025**, *15*, 4037. [\[CrossRef\]](#)

45. Hu, Z.; Jin, R.; Quan, H.; Ni, S.; He, P. A Location Privacy Protection Method Based on Blockchain and Threshold Cryptography. *PLoS ONE* **2025**, *20*, e0324551. [[CrossRef](#)] [[PubMed](#)]
46. Kokaj, A.; Mollakuqe, E. Mathematical Proposal for Securing Split Learning Using Homomorphic Encryption and Zero-Knowledge Proofs. *Appl. Sci.* **2025**, *15*, 2913. [[CrossRef](#)]
47. Singh, S.; Hosen, A.S.M.S.; Yoon, B. Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. *IEEE Access* **2021**, *9*, 13938–13959. [[CrossRef](#)]
48. Dhokrat, J.G.; Pulgam, N.; Maktum, T.; Mane, V. A Framework for Privacy-Preserving Multiparty Computation with Homomorphic Encryption and Zero-Knowledge Proofs. *Informatica* **2024**, *48*, 1–14. [[CrossRef](#)]
49. Ullah, S.; Zheng, J.; Din, N.; Hussain, M.T.; Ullah, F.; Yousaf, M. Elliptic Curve Cryptography; Applications, Challenges, Recent Advances, and Future Trends: A Comprehensive Survey. *Comput. Sci. Rev.* **2023**, *47*, 100530. [[CrossRef](#)]
50. Wong, W.K.; Dong, N.; Dinh, C.M. PQS-BC: Comparative Analysis of NIST Post-Quantum Signatures for Blockchain. *Lect. Notes Comput. Sci.* **2025**, *15564*, 349–369. [[CrossRef](#)]
51. Garms, L.; Paraíso, T.K.; Hanley, N.; Khalid, A.; Rafferty, C.; Grant, J.; Newman, J.; Shields, A.J.; Cid, C.; O'Neill, M. Experimental Integration of Quantum Key Distribution and Post-Quantum Cryptography in a Hybrid Quantum-Safe Cryptosystem. *Adv. Quantum Technol.* **2024**, *7*, 2300304. [[CrossRef](#)]
52. Akkal, M.; Cherbal, S.; Annane, B.; Lakhlef, H.; Kharoubi, K. Quantum, Post-Quantum, and Blockchain Approaches for Securing the Internet of Medical Things: A Systematic Review. *Clust. Comput.* **2025**, *28*, 655. [[CrossRef](#)]
53. Nejatollahi, H.; Shahhosseini, S.; Cammarota, R.; Dutt, N. Exploring Energy Efficient Quantum-Resistant Signal Processing Using Array Processors. In Proceedings of the ICASSP 2020—2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Barcelona, Spain, 4–8 May 2020; pp. 1539–1543. [[CrossRef](#)]
54. Gautam, D.; Prajapat, S.; Kumar, P.; Das, A.K.; Cengiz, K.; Susilo, W. Blockchain-Assisted Post-Quantum Privacy-Preserving Public Auditing Scheme to Secure Multimedia Data in Cloud Storage. *Clust. Comput.* **2024**, *27*, 8159–8172. [[CrossRef](#)]
55. Rammohan, S.R.; Chakravarthi, K.; Sharma, N.; Sharma, S.; Natarajan, M. Systematic Survey on Energy Conservation Using Blockchain for Sustainable Computing Challenges and Roadmaps. *Int. J. Adapt. Control Signal Process.* **2025**, *39*, 247–265. [[CrossRef](#)]
56. Esposito, M.; Tse, T.; Goh, D. Decentralizing Governance: Exploring the Dynamics and Challenges of Digital Commons and DAOs. *Front. Blockchain* **2025**, *8*, 1538227. [[CrossRef](#)]
57. Sharma, T.; Sharma, S.R. Post-Quantum Cryptography for Navigating Challenges and Exploring Opportunities. *Int. J. Res. Rev. Appl. Sci. Humanit. Technol.* **2025**, *2*, 14–21. [[CrossRef](#)]
58. Dekkaki, K.C.; Tasic, I.; Cano, M.-D. Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process. *Technologies* **2024**, *12*, 241. [[CrossRef](#)]
59. Gbaja, C. Designing Quantum-Resilient Data Encryption Protocols for Securing Multi-Cloud Architectures in Critical Infrastructure Networks. *Int. J. Res. Publ. Rev.* **2025**, *6*, 9442–9456. [[CrossRef](#)]
60. Hossain, F.; Hasan, K.; Amin, A.; Mahmud, S. Quantum Machine Learning for Enhanced Cybersecurity: Proposing a Hypothetical Framework for Next-Generation Security Solutions. *J. Technol. Inf. Commun.* **2024**, *4*, 32222. [[CrossRef](#)]
61. Akbar, M.; Waseem, M.M.; Mehanoor, S.H.; Barmavatu, P. Blockchain-Based Cyber-Security Trust Model with Multi-Risk Protection Scheme for Secure Data Transmission in Cloud Computing. *Clust. Comput.* **2024**, *27*, 9091–9105. [[CrossRef](#)]
62. Pasupuleti, M.K. Post-Quantum Cryptography: Algorithms and Implementation Challenges. *Int. J. Acad. Ind. Res. Innov.* **2025**, *5*, 234–243. [[CrossRef](#)]
63. Yi, X.; Wu, D.; Jiang, L.; Fang, Y.; Zhang, K.; Zhang, W. An Empirical Study of Blockchain System Vulnerabilities: Modules, Types, and Patterns. In Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering, Singapore, 14–18 November 2022; pp. 709–721. [[CrossRef](#)]
64. Kuznetsov, O.; Zakharov, D.; Frontoni, E. Deep Learning-Based Biometric Cryptographic Key Generation with Post-Quantum Security. *Multimed. Tools Appl.* **2023**, *83*, 56909–56938. [[CrossRef](#)]
65. Liu, Y.; Tan, T.; Zhuo, Y. Hybrid Consensus Protocols and Security Analysis for Blockchain. In Proceedings of the 2022 International Conference on Data Analytics, Computing and Artificial Intelligence (ICDACAI), Zakopane, Poland, 15–16 August 2022; pp. 191–195. [[CrossRef](#)]
66. Li, N.; Qi, M.; Xu, Z.; Zhu, X.; Zhou, W.; Wen, S.; Xiang, Y. Blockchain Cross-Chain Bridge Security: Challenges, Solutions, and Future Outlook. *Distrib. Ledger Technol. Res. Pract.* **2025**, *4*, 1–34. [[CrossRef](#)]
67. Sezer, B.B.; Akleyek, S.; Nuriyev, U. PP-PQB: Privacy-Preserving in Post-Quantum Blockchain-Based Systems: A Systematization of Knowledge. *IEEE Access* **2025**, *13*, 41382–41405. [[CrossRef](#)]
68. Elkhodr, M. An AI-Driven Framework for Integrated Security and Privacy in Internet of Things Using Quantum-Resistant Blockchain. *Future Internet* **2025**, *17*, 246. [[CrossRef](#)]
69. Venkatachalam, K.; Balamaniandan, A.; Shaik, R.; Karthikayen, A.; Janardhan, S.P.; Venkatesan, M. VLSI-Optimized Post-Quantum Cryptographic Architecture for Secure IoT and Blockchain Applications. *J. VLSI Circuits Syst.* **2025**, *7*, 19–24. [[CrossRef](#)]

70. Baseri, Y.; Chouhan, V.; Hafid, A. Navigating Quantum Security Risks in Networked Environments: A Comprehensive Study of Quantum-Safe Network Protocols. *Comput. Secur.* **2024**, *142*, 103883. [CrossRef]
71. Yesina, M.V.; Ostrianska, Y.V.; Gorbenko, I.D. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. *Radiotekhnika* **2022**, *3*, 75–86. [CrossRef]
72. Joseph, D.; Misoczki, R.; Manzano, M.; Tricot, J.; Pinuaga, F.D.; Lacombe, O.; Leichenauer, S.; Hidary, J.; Venables, P.; Hansen, R. Transitioning Organizations to Post-Quantum Cryptography. *Nature* **2022**, *605*, 237–243. [CrossRef] [PubMed]
73. Wuille, P.; Nick, J.; Towns, A. Taproot: SegWit Version 1 Spending Rules; Bitcoin Improvement Proposal (BIP) 341. 2020. Available online: <https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki> (accessed on 7 June 2026).
74. Lombrozo, E.; Lau, J.; Wuille, P. Segregated Witness (Consensus Layer); Bitcoin Improvement Proposal (BIP) 141. 2015. Available online: <https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki> (accessed on 7 June 2026).
75. Ethereum Foundation. The Merge; Ethereum.org, 2022. Available online: <https://ethereum.org/en/roadmap/merge/> (accessed on 7 June 2026).
76. Bakyt, M.; Spada, L.L.; Zeeshan, N.; Moldamurat, K.; Atanov, S.; Konyrkhanova, A.; Yurkov, N.; Kuanysh, A.; Marat, Y.; Tilenbayev, A. Advanced Cybersecurity Framework for LEO Aerospace: Integrating Quantum Cryptography, Artificial Intelligence Anomaly Detection, and Blockchain Technology. *J. Robot. Control JRC* **2025**, *6*, 695–714. [CrossRef]
77. Okika, N.; Nwatuze, G.A.; Olarinoye, H.S.; Nwaka, A.A.; Igba, E.; Dunee, R. Assessing the Vulnerability of Traditional and Post-Quantum Cryptographic Systems through Penetration Testing and Strengthening Cyber Defenses with Zero Trust Security in the Era of Quantum Computing. *IJISRT* **2025**, *10*, 1240–1258. [CrossRef]
78. Zohaib, M.; Altuwaijri, F.S.; Hyrynsalmi, S. Integrating Quantum Computing and Blockchain: Building the Foundations of Secure, Efficient 6G Technology. In Proceedings of the 1st ACM International Workshop on Quantum Software Engineering: The Next Evolution (QSE-NE '24), Porto de Galinhas, Brazil, 16 July 2024; pp. 27–34. [CrossRef]
79. National Security Agency. *Announcing the Commercial National Security Algorithm Suite 2.0*; CNSA 2.0; NSA: Fort Meade, MD, USA, 2022. Available online: <https://www.nsa.gov/Press-Room/Digital-Media-Center/Document-Gallery/igphoto/2003728741/> (accessed on 28 May 2026).
80. National Institute of Standards and Technology. *Module-Lattice-Based Key-Encapsulation Mechanism Standard*; Federal Information Processing Standards Publication (FIPS) 203; NIST: Gaithersburg, MD, USA, 2024. [CrossRef]
81. National Institute of Standards and Technology. *Module-Lattice-Based Digital Signature Standard*; Federal Information Processing Standards Publication (FIPS) 204; NIST: Gaithersburg, MD, USA, 2024. [CrossRef]
82. National Institute of Standards and Technology. *Stateless Hash-Based Digital Signature Standard*; Federal Information Processing Standards Publication (FIPS) 205; NIST: Gaithersburg, MD, USA, 2024. [CrossRef]
83. NIS Cooperation Group. *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*; European Commission: Brussels, Belgium, 2025.
84. National Cyber Security Centre. *Timelines for Migration to Post-Quantum Cryptography*; NCSC: London, UK, 2025.
85. Institute of Commercial Cryptography Standards. *Next-Generation Commercial Cryptographic Algorithms (NGCC) Program*; Office of the State Commercial Cryptography Administration (OSCCA): Beijing, China, 2025.
86. Hosseini, S.M.; Ferreira, J.; Bartolomeu, P.C. Blockchain-Based Decentralized Identification in IoT: An Overview of Existing Frameworks and Their Limitations. *Electronics* **2023**, *12*, 1283. [CrossRef]
87. Jian, W.Z.; Mammi, H.K. Cryptography for Blockchain System: Comparative Analysis of Cryptographic Algorithms. *Int. J. Innov. Comput.* **2025**, *15*, 131–137. [CrossRef]
88. Deshmukh, S.A.; Kasar, S. Applications of Blockchain Technology in Privacy Preserving and Data Security for Real Time (Data) Applications. *Concurr. Comput. Pract. Exp.* **2024**, *36*, e8277. [CrossRef]
89. Weinberg, A.I.; Petratos, P.; Faccia, A. Will Central Bank Digital Currencies (CBDC) and Blockchain Cryptocurrencies Coexist in the Post Quantum Era? *Discov. Anal.* **2025**, *3*, 8. [CrossRef]
90. Haddouti, S.E.; Kettani, M.D.E.-C.E.; Chaoui, H. Unveiling Blockchain Security and Resilience in the Quantum Age: An Analytical Study of Post-Quantum and Quantum Approaches. In Proceedings of the 2024 7th International Conference on Advanced Communication Technologies and Networking (CommNet), Rabat, Morocco, 4–6 December 2024; pp. 1–8. [CrossRef]
91. Bhuvaneshwari, A.J.; Kaythry, P.; Kishore, R.; MuthuHarish, R. Post-Quantum Enhanced Ascon for Secure Vehicular IoT Data Integrity. *Sci. Rep.* **2025**, *15*, 26591. [CrossRef] [PubMed]
92. Gan, L.; Yokubov, B. A Performance Comparison of Post-Quantum Algorithms in Blockchain. *J. Br. Blockchain Assoc.* **2023**, *6*, 1–10. [CrossRef]
93. Dolev, S.; Guo, B.; Niu, J.; Wang, Z. SodsBC: A Post-Quantum by Design Asynchronous Blockchain Framework. *IEEE Trans. Dependable Secur. Comput.* **2024**, *21*, 47–62. [CrossRef]
94. Spitz, S.; Lawall, A.; Andrzejczak, M. Quantum-Resilient IoT: Integrating Hardware-Based Post-Quantum Cryptography for Robust Device Security. In Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP), Porto, Portugal, 20–22 February 2025; Volume 2, pp. 419–424.

95. Paul, S.; Mazumdar, M.M.; Chakraborty, S. Quantum Resistance Blockchain Algorithm Using QHF and Novel Consensus Mechanism. In Proceedings of the 2025 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 18–19 January 2025; pp. 1–6. [\[CrossRef\]](#)
96. Belchior, R.; Vasconcelos, A.; Guerreiro, S.; Correia, M. A Survey on Blockchain Interoperability: Past, Present, and Future Trends. *ACM Comput. Surv.* **2022**, *54*, 1–41. [\[CrossRef\]](#)
97. Karpinski, M.; Kuznetsov, O.; Oliynykov, R. Security, Privacy, Confidentiality, and Trust in the Blockchain: From Theory to Applications. *Electronics* **2025**, *14*, 581. [\[CrossRef\]](#)
98. Li, S.; Chen, Y.; Chen, L.; Liao, J.; Kuang, C.; Li, K.; Liang, W.; Xiong, N. Post-Quantum Security: Opportunities and Challenges. *Sensors* **2023**, *23*, 8744. [\[CrossRef\]](#) [\[PubMed\]](#)
99. Chaudhry, U.H.; Arshad, R.; Khalid, A.; Ray, I.G.; Hussain, M. Zk-DASTARK: A Quantum-Resistant, Data Authentication and Zero-Knowledge Proof Scheme for Protecting Data Feed to Smart Contracts. *Comput. Electr. Eng.* **2025**, *123*, 110089. [\[CrossRef\]](#)
100. Nguyen, H.; Huda, S.; Nogami, Y.; Nguyen, T.T. Security in Post-Quantum Era: A Comprehensive Survey on Lattice-Based Algorithms. *IEEE Access* **2025**, *13*, 89003–89024. [\[CrossRef\]](#)
101. García, C.R.; Rommel, S.; Takarabt, S.; Olmos, J.J.V.; Guilley, S.; Nguyen, P.; Monroy, I.T. Quantum-Resistant Transport Layer Security. *Comput. Commun.* **2024**, *213*, 345–358. [\[CrossRef\]](#)
102. Ilyas, M.; Cui, S.; Perkowski, M. Ternary Logic Design in Topological Quantum Computing. *J. Phys. Math. Theor.* **2022**, *55*, 305302. [\[CrossRef\]](#)
103. Almotiri, S.H. Quantum-Resilient Software Security: A Fuzzy AHP-Based Assessment Framework in the Era of Quantum Computing. *PLoS ONE* **2024**, *19*, e0316274. [\[CrossRef\]](#) [\[PubMed\]](#)
104. Hamdi, A.; Fourati, L.; Ayed, S. Vulnerabilities and Attacks Assessments in Blockchain 1.0, 2.0 and 3.0: Tools, Analysis and Countermeasures. *Int. J. Inf. Secur.* **2024**, *23*, 713–757. [\[CrossRef\]](#)
105. Bs, L.; Kaulgud, N. Integrating Post-Quantum Cryptography in Transport Layer Security 1.3 for Iot: A Performance Analysis on Resource-Constrained Hardware. In Proceedings of the 2025 Third International Conference on Networks, Multimedia and Information Technology (NMITCON), Bengaluru, India, 1–2 August 2025; pp. 1–8. [\[CrossRef\]](#)
106. Sagingalieva, A.; Kordzanganeh, M.; Kenbayev, N.; Kosichkina, D.; Tomashuk, T.; Melnikov, A. Hybrid Quantum Neural Network for Drug Response Prediction. *Cancers* **2023**, *15*, 2705. [\[CrossRef\]](#) [\[PubMed\]](#)
107. Buser, M.; Dowsley, R.; Esgin, M.F.; Gritti, C.; Kermanshahi, S.K.; Kuchta, V.; LeGrow, J.T.; Liu, J.K.; Phan, R.C.-W.; Sakzad, A.; et al. A Survey on Exotic Signatures for Post-Quantum Blockchain: Challenges and Research Directions. *ACM Comput. Surv.* **2023**, *55*, 251. [\[CrossRef\]](#)
108. Ananthakrishna, V.; Yadav, C.S. QP-ChainSZKP: A Quantum-Proof Blockchain Framework for Scalable and Secure Cloud Applications. *Int. J. Comput. Exp. Sci. Eng.* **2025**, *11*, 162–180. [\[CrossRef\]](#)
109. Dibie, E. Enhancing Cybersecurity for Renewable Energy with Quantum Algorithms and Cloud-Based AI. *J. Adv. Math. Comput. Sci.* **2024**, *39*, 140–151. [\[CrossRef\]](#)
110. Khalid, M.I.; Ehsan, I.; Al-Ani, A.K.; Iqbal, J.; Hussain, S.; Ullah, S.S.; Nayab. A Comprehensive Survey on Blockchain-Based Decentralized Storage Networks. *IEEE Access* **2023**, *11*, 10995–11015. [\[CrossRef\]](#)
111. Shevchuk, R.; Martsenyuk, V.; Adamyk, B.; Benson, V.; Melnyk, A. Anomaly Detection in Blockchain: A Systematic Review of Trends, Challenges, and Future Directions. *Appl. Sci.* **2025**, *15*, 8330. [\[CrossRef\]](#)
112. Cui, W.; Dou, T.; Yan, S. Threats and Opportunities: Blockchain Meets Quantum Computation. In Proceedings of the 2020 39th Chinese Control Conference (CCC), Shenyang, China, 27–29 July 2020; pp. 5822–5824. [\[CrossRef\]](#)
113. Rasappan, S.; Kumaravel, S.K.; Sambas, A.; Moghrabi, I.A.R.; Sulaiman, I.M.; Hassan, B.A. A Novel Chua's Based 2-D Chaotic System and Its Performance Analysis in Cryptography. *PLoS ONE* **2024**, *19*, e0306818. [\[CrossRef\]](#) [\[PubMed\]](#)
114. Taherdoost, H.A. Critical Review of Blockchain Acceptance Models—Blockchain Technology Adoption Frameworks and Applications. *Computers* **2022**, *11*, 24. [\[CrossRef\]](#)
115. Thanalakshmi, P.; Rishikesh, A.; Marceline, J.M.; Joshi, G.P.; Cho, W. A Quantum-Resistant Blockchain System: A Comparative Analysis. *Mathematics* **2023**, *11*, 3947. [\[CrossRef\]](#)
116. Karakaya, A.; Ulu, A. A Review on Latest Developments in Post-Quantum Based Secure Blockchain Systems. In Proceedings of the 2023 11th International Symposium on Digital Forensics and Security (ISDFS), Chattanooga, TN, USA, 11–12 May 2023; pp. 1–6. [\[CrossRef\]](#)
117. Yan, H.; Hu, H.; Ye, Q.; Xu, J. Multi-Hop Sanitizable Signature for Collaborative Edge Computing. *J. Comput. Secur.* **2025**, *33*, 79–99. [\[CrossRef\]](#)
118. Gomes, J.; Khan, S.; Svetinovic, D. Fortifying the Blockchain: A Systematic Review and Classification of Post-Quantum Consensus Solutions for Enhanced Security and Resilience. *IEEE Access* **2023**, *11*, 74088–74100. [\[CrossRef\]](#)
119. Zheng, X. Research on Blockchain Smart Contract Technology Based on Resistance to Quantum Computing Attacks. *PLoS ONE* **2024**, *19*, e0302325. [\[CrossRef\]](#) [\[PubMed\]](#)
120. Yi, H. Secure Social Internet of Things Based on Post-Quantum Blockchain. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 950–957. [\[CrossRef\]](#)

121. Varadala, S.; Xu, H. A Blockchain-Enabled Decentralized Zero-Trust Architecture for Anomaly Detection in Satellite Networks via Post-Quantum Cryptography and Federated Learning. *Future Internet* **2025**, *17*, 516. [CrossRef]
122. Niu, C.; Wei, B.; Huang, Z.; Yang, Z.; Hong, C.; Wang, M.; Wei, T. SoK: FHE-Friendly Symmetric Ciphers and Transciphering. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2025**, 2025, 583–613. [CrossRef]
123. Turbé, H.; Bjelogrić, M.; Lovis, C.; Mengaldo, G. Evaluation of Post-Hoc Interpretability Methods in Time-Series Classification. *Nat. Mach. Intell.* **2023**, *5*, 250–260. [CrossRef]
124. Kop, M. Establishing a Legal-Ethical Framework for Quantum Technology. Yale Journal of Law & Technology (YJoLT) Blog, Authored on Tuesday, 30 March 2021. Available online: <https://yjolt.org/blog/establishing-legal-ethical-framework-quantum-technology> (accessed on 28 May 2026).
125. Grimsley, H.R.; Economou, S.E.; Barnes, E.; Mayhall, N.J. An Adaptive Variational Algorithm for Exact Molecular Simulations on a Quantum Computer. *Nat. Commun.* **2019**, *10*, 3007. [CrossRef] [PubMed]
126. Lopez, J.; Cadena, V.; Rahman, M.S. Evaluating Post-Quantum Cryptographic Algorithms on Resource-Constrained Devices. In Proceedings of the 2025 IEEE International Conference on Quantum Computing and Engineering (QCE), Albuquerque, NM, USA, 31 August–5 September 2025; Volume 2, pp. 655–656. [CrossRef]
127. Faheem, M.; Al-Khasawneh, M.A.; Khan, A.A.; Madni, S.H.H. Cyberattack Patterns in Blockchain-Based Communication Networks for Distributed Renewable Energy Systems: A Study on Big Datasets. *Data Brief* **2024**, *53*, 110212. [CrossRef] [PubMed]
128. Dhar, S.; Khare, A.; Dwivedi, A.D.; Singh, R. Securing IoT Devices: A Novel Approach Using Blockchain and Quantum Cryptography. *Internet Things* **2024**, *25*, 101019. [CrossRef]
129. Adejumo, A.P.; Ogburie, C.P. The Role of Cybersecurity in Safeguarding Finance in a Digital Era. *World J. Adv. Res. Rev.* **2025**, *25*, 1542–1556. [CrossRef]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.