A Work Project, presented as part of the requirements for the Award of a Master's degree in Impact Entrepreneurship & Innovation from the Nova School of Business and Economics.

The vulnerability of blockchain technology to quantum computing as seen by the scholars: a systematic literature review and bibliometric analysis

Florine Shifra Elskamp – 68345

Work project carried out under the supervision of:

Leid Zejnilovic

12/12/2025

Abstract

Blockchain technology's cryptographic foundations face threats from advancing quantum computing, mainly through Shor's and Grover's algorithms. In this work project, we conduct a systematic literature review and bibliometric analysis, to review the knowledge on the risk of the development of quantum computing for blockchain technology. In particular, we review the publications from 2019 to 2025 across Scopus and EBSCO to identify the research themes. While theoretical research is advancing, the reviewed literature reveals a scarcity of studies documenting practical implementation, standardization, and governance frameworks. This study identifies the need for efforts in developing transition roadmaps and frameworks, to assess crypto agility.

Keywords: Blockchain security, quantum computing, post-quantum cryptography, systematic literature review

Funding statement: This work used infrastructure and resources funded by the Ripple Blockchain Initiative.

List of Abbreviations

Quantum Computing	**QC**
Harvest now, decrypt later	**HNDL**
Post-quantum cryptography	**PQC**
Distributed ledger technology	**DLT**

List of Figures

List of Tables

1 Introduction

The backbone of Blockchain systems is encryption; they rely on different cryptographic techniques, which shaped the way trust and verification operate in decentralized networks (Fernández-Caramés & Fraga-Lamas, 2020). In 2008, since the release of Bitcoin, distributed ledgers have been built around algorithms such as the Elliptic Curve Digital Signature Algorithm (ECDSA), Riven-Shamir-Adlerman (RSA) and Secure Hash Algorithm 256 (SHA-256). While RSA relies on the computational difficulty of factoring large prime numbers, ECDSA derives its security from the algebraic structure of elliptic curves. These digital signature schemes serve as the primary mechanism for authenticating transactions and verifying user identities (Nakamoto, 2008). SHA-256 utilizes one-way mathematical functions to condense data into a fixed unique fingerprint, ensuring the integrity of the ledger history. The mechanisms serve distributed ledgers well, but are facing issues due to the development of quantum computers. (Aggarwal et al., 2018).

The debate about quantum computing has shifted from speculations to practical questions of security readiness of blockchain projects (Allende et al., 2023). Although large-scale, fault-tolerant quantum computers are not yet available, several technology and finance companies, including IBM, Google, Microsoft, AWS, and JPMorgan, are actively developing quantum hardware or collaborating on quantum-based research (Egger et al., 2020). At the same time, firms like D-Wave and IonQ have introduced specialized quantum systems, adding momentum to the broader field (Preskill, 2018).

The concern about blockchain's vulnerability to quantum computing stems primarily from the capabilities of algorithms like Shor's and Grover's, which undermine the mathematical assumptions that keep current cryptographic systems secure. Shor's algorithm threatens public-

key cryptography by enabling efficient solutions to the discrete logarithm and factorization problems (Shor, 1997). Functionally, this breaks the digital signature schemes (like ECDSA) used to authenticate transactions, meaning an attacker could derive private keys from public keys to forge signatures and steal funds. While Grover's algorithm reduces the effective security of hash-based system (Grover, 1996). For blockchain, this weakens the resistance of hashing algorithms (like SHA-256) against brute-force attacks, drastically lowering the computational difficulty required to mine blocks or manipulate the ledger history. Combined with the "harvest now, decrypt later" (HNDL) the implications for long-lived, immutable ledgers are serious. The HNDL threat is a threat where publicly visible blockchain data can be collected today and decrypted once quantum computers mature (Rajan & Visser, 2019) (York, 2023).

This threat is particularly acute for systems that are designed to be immutable, as past compromises cannot be purged from the ledger (Fernández-Caramés, 2019).

Despite overwhelming consensus on the existential threat posed by quantum computers on blockchain technology, as algorithms like Shor's algorithm and Grover's algorithm efficiently dismantle the ECDSA and RSA cryptography underpinning nearly all major DLT transactions (Kiktenko et al., 2018), there is a gap between this theoretical certainty and strategic (Yin et al., 2018), actionable readiness (Alagic et al., 2022). To address this gap, we first need to establish the state of the art, a task that constitutes the essence of this work. Therefore, we define the following Research Question:

What is the current state of academic and technical literature regarding the vulnerability of blockchain technology to quantum computing?

To respond to this question, we conduct a systematic literature review and bibliometric analysis. While multiple literature reviews have been published recently, they primarily focus

on technical cryptographic feasibility rather than organizational adoption. This study addresses that gap by shifting the focus from what the technology is to how organizations must adapt.

We map existing research, identify where academic attention is concentrated, and where practical guidance is still lacking. In doing so, the aim is to make the technical discourse accessible to readers who do not specialize in cryptography but are interested in blockchain's long-term resilience (Esgin et al., 2021).

2 Methods

The intention of this study is to capture not only the main themes in the literature but also the structure of the research landscape and how it has evolved. The qualitative approach of a Systematic Literature Review (SLR) is enriched with the quantitative power of Bibliometric Analysis (BA). This approach initially involves an SLR to systematically identify, assess, and synthesize the relevant academic literature concerning the impact of Quantum computing on Blockchain security (Snyder, 2019). Subsequently, the BA is applied to the selected papers, utilizing network metrics to generate descriptive findings (Donthu et al., 2021). Ultimately, this combination of SLR and BA guarantees both a qualitative synthesis and a statistically informed mapping of the research landscape, ensuring depth, breadth, and clarity in identifying both foundational knowledge and future research trajectories.

2.1 Systematic literature analysis

The seed papers were gathered from Scopus and EBSCO, chosen because both provide reliable metadata for quantitative follow-up. The search was limited to English-language publications from 2019 to 2025 in Business and Economics. Books and chapters were excluded to maintain consistency. Multiple search queries were tested. The following two search queries provided the broadest coverage or results:

1. (KEY("Blockchain") AND ALL FIELDS("Post-quantum cryptography"))

2. (KEY("Post-quantum cryptography") AND ALL FIELDS(“Blockchain”))

The search queries specifically utilized the term 'Post-quantum cryptography' (PQC) rather than the broader 'Quantum Computing' to filter the dataset for implications rather than general quantum theory. While searching for 'Quantum Computing' would result in a higher volume of results, it introduces significant noise, including papers on quantum hardware development and quantum physics. With these queries SCOPUS returned 73 and 25 results (with 9 duplicates), and EBSCO 4. Filtering proceeded in three stages.

- Initial screening: removal of duplicates and papers with missing metadata.
- Abstract check: assessment of relevance and confirmation that the full text was available.
- Full-text review: evaluation of the paper’s alignment with the research question.

A PRISMA diagram (Figure 1) documents each stage of this selection process (Snyder, 2019). After filtering, 27 papers remained and formed the seed dataset. AI-assisted tools, such as SciSpace, Gemini, and Elicit, were tested to support data extraction and identify preliminary clusters, although final judgments were made manually. Appendix 1 provides the full list of papers used in this analysis, organized by their designated PaperID for ease of reference. In this report PaperID is presented as [PaperID].

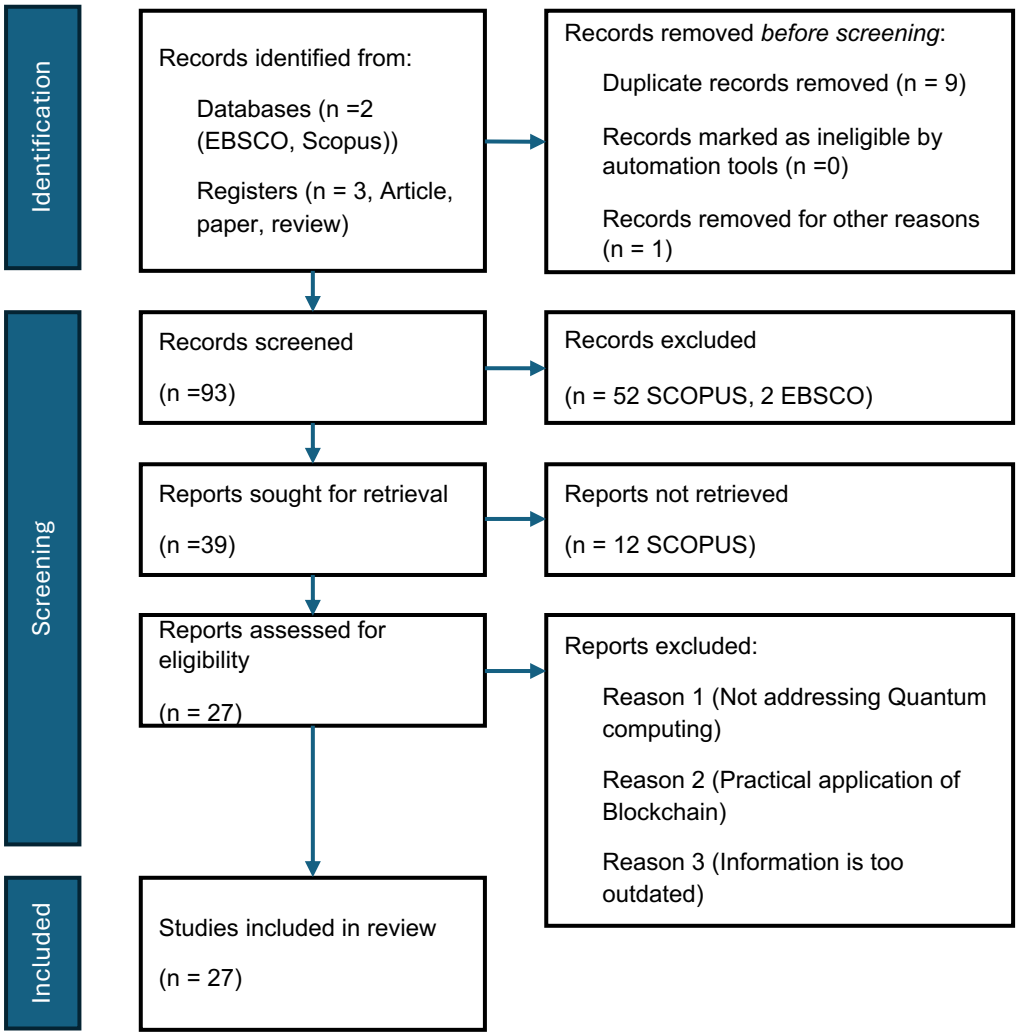


Figure 1: PRISMA

2.2 Bibliometric analysis

The bibliometric analysis includes a performance analysis and science mapping (Donthu et al., 2021). The performance analysis is done to identify publication trends in the research area, identify most productive sources, find key contributors and understand the geographical and institutional contribution. To perform these analysis Microsoft Excel/ Power Query and SciSpace has been leveraged due to its user friendliness and comprehensive functionalities. The performance analysis is enhanced with a science mapping which gives insight into thematic clusters, co-citations, research fronts and collaboration networks. For the co-citation analysis the references are extracted resulting in a set of 1427 entries (929 unique). For co-citation analysis, only sources cited in more than two papers were retained, yielding a

condensed network of 44 references, revealing 5 distinct research clusters and 163 significant co-citation relationships.

3 Bibliometric analysis

The Bibliometric approach is divided into two sections: Performance and Science mapping.

3.1 Performance mapping

The performance mapping consists of publication trends, Most influential sources, author and country contribution.

3.1.1 Trends

Using the final set of 27 papers from the systematic review, the publication timeline reveals a field that has grown steadily but unevenly. Research output fluctuates between 2019 and 2025, with two notable deviations: a dip in 2022, followed by an increase in 2025. Nearly half of all papers (44%) were published in 2024 - 2025, suggesting that the topic has gained momentum in the last two years of the dataset. This rise coincides with heightened global discourse around cryptographically relevant quantum computing and the institutional push for post-quantum cryptography standards.

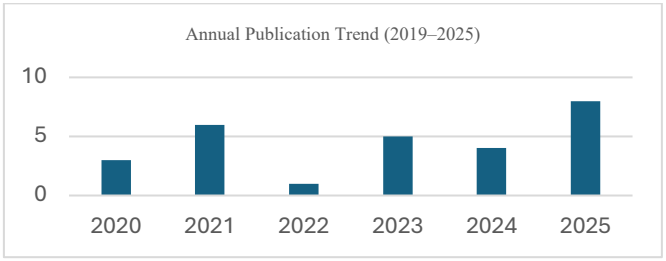


Figure 2: Annual publication trend distribution

3.1.2 Most influential sources

The 27 papers derive from 20 different publication outlets, reflecting the interdisciplinary nature of blockchain-quantum research. Based on a combination of publication count and citation volume, *IEEE Transactions on Engineering Management* emerges as the most influential source, contributing three papers and accumulating the highest citation count (150).

Other journals contribute more selectively but with meaningful impact. For example, *Journal of Open Innovation: Technology, Market, and Complexity* appear only once in the dataset, yet the included article has been cited 86 times. *Business Source Ultimate* hosts four papers, which together accumulate 35 citations.

Overall, the distribution suggests that while a few journals anchor the field, much of the research is dispersed across broader technology and innovation outlets rather than a single disciplinary home.

3.1.3 Author contributors

Most authors in the dataset contribute to only one paper, indicating a relatively dispersed research community. One exception is Yi H., who has authored or co-authored two papers with a combined citation count of 22 (Yi, 2023; Yi et al., 2021). Most papers have been co-authored, 23 papers, and the minority of 4 papers has been sole-authored. The mix between single-authored and collaboratively written work illustrates the multi-disciplinary character of quantum-resilient blockchain research, which often requires expertise across multiple industries.

3.1.4 Country contribution

The 27 papers represent work from authors across 17 countries. A substantial share (19 of 27 papers) involves some form of international collaboration. When total publications (counting contributions from all collaborating countries) are considered, India, China, the United States, Canada, Kazakhstan, and the United Kingdom form the core contributors, jointly accounting for 40 of the 51 country-level contributions. The remaining 11 countries collectively account for the remaining 11 contributions. This distribution suggests an emerging but geographically concentrated research landscape, where a small group of countries currently drives the majority of scholarly output.

3.2 Science mapping

Science-mapping techniques help identify how concepts and references circulate within the field.

3.2.1 Co-word analysis of author keywords

Keywords across the dataset naturally cluster around themes such as blockchain, distributed ledger technologies, quantum cryptography, authentication, and general information security, as shown in Table 1. The most frequently occurring keyword pairings include "blockchain and quantum computing," "authentication and blockchain," and "blockchain and quantum cryptography." While the prevalence of "blockchain", "post-quantum cryptography" and "quantum computing" is expected given the search parameters, Terms as "authentication," "cryptocurrency," provide a clearer picture of researchers' focal points, suggesting potential thematic clusters.

Keyword combination	*Frequency*
blockchain, quantum computing	11
authentication, blockchain	9
blockchain, quantum cryptography	6
authentication, quantum computing	6
blockchain, public key cryptography	5
blockchain, post quantum	5
authentication, quantum cryptography	5
blockchain, cryptocurrency	5
post quantum, quantum cryptography	4
quantum computing, quantum cryptography	4
blockchain, hash function	4
authentication, post quantum	4

Tabel 1: Keywords

3.2.2 Citation analysis

The citation analysis uses Python code generated by SciSpace, an AI platform for searching, understanding and analyzing scientific research papers.

The citation analysis highlights a small number of foundational papers that are repeatedly cited together, presented in Table 2. These works are considered as most influential work withing this study.

Title	Author	# Cited
Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography	(Fernández-Caramés & Fraga-Lamas, 2020)	11
A Fast Quantum Mechanical Algorithm for Database Search	(Grover, 1996)	6
"Algorithms for quantum computation: discrete logarithms and factoring"	(Shor, 1997)	5
Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer	(Shor, 1997)	5
A method for obtaining digital signatures and public-key cryptosystems	(Rivest R, 1978)	4

Tabel 2: Most influential work

This mix reflects the interdisciplinary basis of the field: contemporary blockchain research relies heavily on both the cryptographic foundations established decades ago and the newer quantum-computing developments that challenge those foundations.

For identifying research fronts a hierarchical clustering algorithm is used. This approach allows thematic clusters to emerge from the network structure (Donthu et al., 2021). The analysis identified five distinct research communities with varying sizes and citation impacts. Cluster 1 addresses Post-Quantum Blockchain Security (n=6) with the highest impact of 4 average citations. Key contributions in this group explore post-quantum cryptography implementations, network coding, and quantum key distribution. Cluster 2 is the largest one, with the research on Foundational Quantum and Cryptographic Algorithms (n=30). These works have an average citation of 2,73 and focus on Grover's algorithm, Shor's algorithm, RSA systems, and lattice-based signatures. Cluster 3 has one document about Specialized Applications with 2 citations. Cluster 4 covers Blockchain Technology and Economics (n=3) with 2,67 average citations. The research highlights blockchain adoption, financial transformation, and energy requirements. Cluster 5 is on Blockchain Consensus and Distributed Systems (n=4) with an

average of 2,25 citations. This community prioritizes surveys on consensus mechanisms and distributed ledger technology reviews.

Co-citations networks

The literature shows a strong co-citation between technology transformation and energy consumption studies. Appendix 2 shows the co-citations (edges) between the 44 reference papers (nodes). The following pairs of works are most frequently cited together, indicating strong intellectual connections:

- Foundational quantum algorithms often cited together, (Grover, 1996; Shor, 1997).
- Linking quantum threats to blockchain security solutions (Fernández-Caramés & Fraga-Lamas, 2020)
- Quantum algorithms threatening classical cryptography (Grover, 1996), (Rivest R, 1978).

In general, there are multiple co-citations with theoretical quantum computing and Quantum Computing Foundations.

4 Systematic literature analysis

The systematic literature analysis is organized into two parts, according to the guidelines of a SLR (Snyder, 2019). The first part provides a descriptive analysis of the methods and orientations used in the reviewed papers. The second examines the recurring themes that emerge once the content is grouped according to shared focus areas. Together, these findings offer a picture of how the research community approaches the quantum threat to blockchain systems and where its efforts are concentrated.

4.1 Descriptive Analysis

To compare the methodologies and research styles used across the 27 papers, the studies were classified into six categories. Their distribution reveals the developmental stage of the field.

Technical/conceptual papers form the largest group (37%), many of which focus on core cryptographic issues or outline the theoretical foundations of quantum risks. Another substantial portion (22%) falls into the design science/implementation category, where authors test or prototype post-quantum methods on blockchain platforms. This 59% combined share of solution-oriented research indicates that researchers and practitioners recognize the quantum threat to blockchain as an imminent rather than distant concern, prompting urgent development of cryptographic alternatives and architectural adaptations.

The presence of four literature reviews (15%) indicates that the field has matured enough to require synthesis and consolidation of its expanding knowledge base [6,7,10,11]. Yet this synthesis occurs alongside ongoing conceptual work, suggesting that the field has not yet reached consensus. Researchers are still exploring multiple competing approaches to quantum-resistant blockchain design rather than converging on standardized solutions.

The limited representation of strategic/policy analysis (11%) and risk/impact analysis (11%) papers reveals a significant methodological gap with important implications for the field's practical relevance. While technical solutions dominate the area, questions of governance, adoption barriers, migration strategies, and organizational readiness remain underexplored. This imbalance could be problematic: technically suitable solutions may fail without adequate attention to implementation costs, regulatory frameworks, stakeholder coordination, and change management. The near-absence of empirical qualitative studies examining real-world adoption challenges or stakeholder perspectives further reinforces this gap. The field remains heavily driven by computer science and cryptography communities, with insufficient engagement from business, economics, and policy scholars who could address the sociotechnical dimensions of quantum-resistant blockchain transition.

When viewed over time, publication activity increases notably from 2023 onward. This corresponds with the expert prediction and broader awareness that large-scale, fault-tolerant quantum machines may arrive sooner than originally projected. It also parallels the momentum generated by post-quantum cryptography standardization efforts, such as NIST's multi-year evaluation process. As standards stabilize, research naturally shifts toward implementation studies and transition planning, which is reflected in the more recent papers focusing on prototypes, performance testing, and migration frameworks (Alagic et al., 2022).

In summary, the methodological landscape suggests that the field is progressing beyond early conceptual debates but has not yet reached a stable, unified set of practices. Technical work remains the dominant area of focus, while strategic, economic, and governance questions are still at the margins.

4.2 Thematic clusters

A thematic review of the selected papers reveals five major clusters:

1. Post-quantum cryptographic solutions (15 papers)
2. Implementation & performance evaluation (13 papers)
3. Domain-specific quantum safe blockchain applications & use cases (12 papers)
4. Quantum threat assessment & vulnerability analysis (9 papers)
5. Governance, trust & strategic considerations (7 papers)

The themes overlap, with many papers contributing to multiple thematic areas, which reflects the sociotechnical nature of quantum-resilient blockchain research, spanning technical, economic, and organizational domains. Nevertheless, the five themes outlined below offer a structured view of the core research directions.

Cluster 1: Post-quantum cryptographic solutions

The literature demonstrates widespread consensus that current blockchain cryptographic foundations, ECDSA and SHA-256 hashing, face threats from Shor's and Grover's quantum algorithms, driving urgent development of quantum-resistant alternatives [4,7,9,12,13,14,16,17,18,20,21,23,25,26,27]. Researchers have converged on three primary cryptographic families as viable replacements: lattice-based cryptography [4,12,14,16,17,21,25], hash-based signatures [7,20,26], and code-based cryptography [7,13,23]. Lattice-based approaches are receiving the most attention due to their balance between security assumptions and computational efficiency. However, significant disagreement persists regarding optimal implementation strategies, particularly concerning the trade-off between security margins and performance issues [4,16,21,25].

Multiple studies propose concrete post-quantum signature schemes- the cryptographic mechanisms used to authorize transactions on the blockchain- for blockchain contexts, with lattice-based solutions like Dilithium and Falcon emerging as frontrunners [16,21,25], Yet these introduce signature sizes 10-50 times larger than current ECDSA signatures, creating blockchain bloat concerns that remain unresolved [4,20,25]. Hash-based signatures, particularly XMSS (extended Merkle Signature Scheme), offer proven security based on minimal cryptographic assumptions but suffer from statefullness requirements that conflict with blockchain's distributed architecture [7,20,26]. The literature highlights a tension: while NIST's post-quantum standardization process has identified candidate algorithms [7,16,21], their direct integration into existing blockchain protocols proves more complex than initially anticipated, with several papers documenting significant compatibility challenges when implementing quantum-resistant cryptography in systems designed around classical assumptions [20,21,25].

An emerging area is hybrid cryptographic approaches that combine classical and post-quantum algorithms during transition periods, providing backward compatibility while establishing

quantum resistance [21,25,27]. However, papers diverge sharply on implementation timelines; some advocate immediate migration to post-quantum standards [16,20,23], while others recommend phased transitions that balance urgency against the risk of premature standardization before quantum computing capabilities fully materialize [7,21,27].

Notably absent from most technical proposals is consideration of key management complexity. Post-quantum cryptography introduces substantially larger key sizes and more complex key generation processes that may strain existing blockchain key management practices [17,21].

Cluster 2: Implementation & performance

Empirical evaluation studies reveal that post-quantum cryptographic integration imposes substantial performance penalties across multiple blockchain dimensions, though the severity varies by algorithm choice and implementation approach [4,6,7,9,10,12,16,18,19,21,24,25,27]. By implementing post-quantum computing, transaction sizes expand by 30-400% due to larger signatures and public keys, directly impacting blockchain storage requirements and network bandwidth consumption [4,16,21,25,27]. These overheads create a critical tension: networks prioritizing decentralization and accessibility face greater challenges adopting post-quantum cryptography than permissioned enterprise blockchains with controlled infrastructure [4,21,24].

Real-world implementations report mixed results regarding throughput impact. Some studies document transaction throughput reductions of 40-60% when deploying post-quantum signatures on Ethereum-like platforms [16,21,27], while others achieve throughput degradation below 20% through optimized implementations and algorithm-specific tuning [4,24,25]. This variation suggests that implementation quality and algorithm selection matter as much as inherent cryptographic properties, yet standardized benchmarking frameworks remain absent from the literature, making cross-study comparisons difficult [6,7,24]. Several studies identify computational asymmetry as a critical consideration, signature verification (performed by all

nodes) proves more computationally intensive for some post-quantum schemes than signature generation (performed once by the transaction originator), inverting the cost structure of classical ECDSA and potentially favoring different algorithm choices than initially anticipated [16,21,25].

Another area of implementation research examines migration strategies for transitioning existing blockchains to quantum resistance without hard forks or chain splits [18,21,27]. These studies propose gradual address format transitions, dual-signature periods where both classical and post-quantum signatures coexist, and backward-compatible protocol upgrades [21,27]. However, there is a fundamental disagreement about whether migration should prioritize minimizing disruption to existing users [21,27] or maximizing security through clean-break transitions that force rapid adoption [16,18]. Performance evaluation studies also expose a critical gap: most don't focus on the transition period, leaving unclear how networks will manage the computational and storage overhead of supporting both classical and post-quantum cryptography simultaneously during migration [21,24,27].

Cluster 3: Domain-specific applications & use cases

The literature demonstrates that quantum vulnerability manifests differently across blockchain application domains, with security requirements, performance constraints, and adoption barriers varying substantially by use case [2,3,9,10,12,13,14,15,17,18,19,27]. One of the use cases is E-voting systems. They emerge as a critical application where quantum threats demand immediate attention due to long-term ballot secrecy requirements; votes cast today must remain confidential for decades. Yet current blockchain-based e-voting implementations rely on cryptography that may become quantum-vulnerable within that timeframe [9,18,19].

Supply chain and IoT applications face distinct quantum challenges due to resource constraints of edge devices that may lack computational capacity for post-quantum cryptography

[3,12,14,15,17]. Proposed solutions include using lightweight algorithms or delegating cryptographic operations to more powerful 'fog' or gateway nodes [12,14,17]. However, this delegation approach introduces new trust assumptions that potentially undermine blockchain's decentralization benefits [14,17]. Supply chain applications also highlight the longevity problem: products with multi-decade lifecycles tracked on blockchain require cryptographic protection that remains secure far into the future, yet current post-quantum standards may themselves become obsolete as quantum computing advances [15,17].

Financial applications, including CBDCs (Central Bank Digital Currencies) and DeFi (Decentralized Finance), receive growing attention as quantum-vulnerable high-value targets [2,10,15,27]. These applications face unique challenges: regulatory compliance requirements may mandate specific cryptographic standards, potentially conflicting with post-quantum algorithm choices [15,27]; high transaction volumes make performance overhead particularly costly [10,27]; and systemic risk concerns require coordinated quantum-resistance upgrades across interconnected protocols [10,15]. Several papers argue that financial applications should serve as early adopters driving post-quantum blockchain development due to their high security stakes and centralized governance structures that facilitate coordinated upgrades [10,15,27], while others state that adoption of immature post-quantum standards could create new systemic vulnerabilities [2,15].

Cluster 4: Quantum threat assessment & vulnerability analysis

The literature in this cluster confirms the dual threat model established in the introduction: papers consistently identify asymmetric cryptography (wallets, signatures) as vulnerable to Shor's algorithm [2,5,8,9,10,11,15,23,27], while symmetric hashing is considered weakened but manageable under Grover's algorithm [8,10,11,23]. However, papers diverge significantly on threat timeline assessments. Early papers (2020-2021) projected quantum threats as 15–30-

year concerns [2,5,8], while more recent work (2023-2025) argues that cryptographically relevant quantum computers may emerge within 5-10 years, necessitating immediate action given the long deployment cycles of cryptographic standards [10,15,23,27]. This compression reflects advances in quantum hardware development and growing awareness of "harvest now, decrypt later" attacks, in which adversaries collect encrypted blockchain data today for future quantum decryption [10,15,23].

Risk assessment papers identify cryptocurrency wallets as the most vulnerable blockchain component, particularly addresses with exposed public keys from prior transactions, which become crackable once quantum computing power becomes available [8,9,11,23]. The literature indicates that proof-of-work consensus mechanisms face less severe quantum threats than signature schemes. Grover's algorithm could break consensus security of hash functions [8,11]. However, there seem to be a disagreement on whether proof-of-stake systems face heightened quantum vulnerability due to their heavier reliance on digital signatures for validator authentication. Naik et al. [10] argues that Proof-of-Stake faces heightened risks due to its structural dependence on digital signatures for validator authentication, which are vulnerable to Shor's algorithm. In contrast, Alfaw et al.[11] and Seol and Kim[23] emphasize the fragility of Proof-of-Work systems, focusing on how quantum algorithms weaken hash functions and facilitate 'Quantum 51% attacks' that compromise network control. An underexplored but critical dimension identified by recent papers involves systemic risk amplification in interconnected blockchain ecosystems [10,15,27]. These studies argue that quantum vulnerability assessment must extend beyond individual blockchain security to consider cross-chain bridges, wrapped tokens, and DeFi protocols where quantum attacks on one component could cascade across entire ecosystems [10,15].

Several papers note that quantum computing could enable previously impractical attacks on blockchain governance mechanisms, smart contract platforms, and privacy protocols [9,11,15,27], though these interactions remain insufficiently characterized.

Cluster 5: Governance, trust & strategic considerations

Technical quantum-resistance solutions prove necessary but insufficient for blockchain ecosystem survival. A successful transition requires addressing governance coordination problems, trust dynamics, and strategic adoption incentives [1,2,10,15,18,22,27]. Papers in this cluster identify a critical collective action problem: decentralized blockchain networks lack central authorities to mandate quantum-resistant upgrades, yet individual rational actors may delay costly migrations until quantum threats materialize, creating systemic vulnerability through coordination failure [1,15,22,27]. This governance challenge proves particularly acute for permissionless blockchains like Bitcoin and Ethereum where protocol changes require broad community consensus and backward compatibility concerns constrain design options [22,27].

Trust dynamics complicate quantum-resistant transitions in multiple [1,2,10,18,22]. First, post-quantum cryptographic algorithms rest on newer foundations than classical cryptography, creating uncertainty about long-term security guarantees that may erode user confidence during migration periods [1,2,10]. Second, the transition process itself introduces trust vulnerabilities, hybrid systems supporting both classical and quantum-resistant cryptography expand attack surfaces and create ambiguity about which security properties hold during migration [18,22]. Third, quantum resistance requires users to trust that cryptographic standards selected will remain secure against future quantum advances, yet the literature documents substantial uncertainty about quantum computing development trajectories [2,10,22,27].

Strategic timing considerations generate significant disagreement in the literature [1,2,10,15,22,27]. Some papers argue that early quantum-resistant adoption provides competitive advantage,

positioning blockchains as secure long-term platforms and attracting security-conscious users and institutional adoption [10,15,27]. Others contend that premature migration imposes unnecessary costs and risks [2,22]. The literature also identifies first-mover disadvantages: early adopters bear higher costs and greater risk of selecting algorithms that prove suboptimal, while late movers benefit from learning but face greater quantum vulnerability during the waiting period [1,15,22]. This creates strategic dilemmas where rational actors prefer to free-ride on others' experimentation, potentially resulting in inadequate ecosystem-wide preparation [15,22]. Policy and regulatory dimensions remain underexplored but emerge as critical in recent papers [10,15,22,27]. Several studies argue that government mandates or regulatory incentives may prove necessary to overcome coordination failures and accelerate quantum-resistant adoption, particularly for critical infrastructure and financial applications [15,22,27]. The CBDC literature particularly emphasizes regulatory considerations, noting that central banks possess both strong incentives for quantum resistance (maintaining monetary system integrity) and governance capacity to mandate upgrades [27], potentially positioning CBDCs as catalysts for broader blockchain quantum-resistance adoption.

5 Research gaps

While the reviewed literature offers substantial technical insight, several areas remain underdeveloped. These gaps are not merely academic; they highlight key barriers to preparing blockchain ecosystems for quantum disruption.

A primary deficiency lies in the absence of comprehensive migration frameworks. The literature review shows that most research efforts concentrate on cryptographic feasibilty. Given that NIST has published standardized key algorithms and the 'Harvest Now, Decrypt Later' threat necessitates early intervention, the literature’s failure to address governance coordination and transition strategies represents a gap in organizational readiness.

Jin [22] and Weinberg et al. [27] highlight a critical gap in governance processes, while Rehman et al. [1] and Yoon et al. [15] note that issues of stakeholder alignment, cost distribution, and user communication remain largely unaddressed. Given that blockchain upgrades often involve complex political negotiations, this lack of applied guidance poses a major constraint.

There is also a shortage of empirical research on how actual operators (miners, validators, exchanges, wallet providers) perceive quantum risks. Without real-world data, assumptions about incentives and behavior remain speculative.

Beyond governance challenges, the literature lacks a thorough analysis of costs and business models. The literature measure performance penalties (larger keys, slower verification), but very few convert these findings into operational or financial implications. Absent are analyses of who bears costs versus who captures benefits in decentralized systems [15,22]. The literature neglects business model implications, which leaves questions like: "how do blockchain-based enterprises justify quantum-resistance investments to shareholders, and what competitive dynamics emerge between quantum-resistant and non-resistant platforms?".

These practical questions remain unanswered, even as industry interest in blockchain continues to grow. Finally, a significant oversight exists regarding cross-chain dependencies. Today, blockchain environments are deeply interconnected: bridges, wrapped assets, and multi-chain smart contracts link various networks [10,15]. Yet, the literature tends to analyze vulnerability at the level of individual blockchains. There is little to no work addressing what happens when a quantum attack compromises one system in a networked chain of dependencies.

This oversight is significant. A single point of cryptographic weakness could trigger broader failures across multiple platforms. A cross-chain perspective is essential but currently lacking.

6 Conclusions

The review reveals a technically advanced but strategically immature landscape. Research heavily favors cryptographic solutions, specifically lattice-based algorithms, but neglects the governance and migration frameworks required for actual adoption. A critical shift in the literature shortens the predicted quantum threat timeline from decades to 5–10 years, necessitating immediate operational planning. Furthermore, current studies largely ignore systemic risks in interconnected blockchain ecosystems, such as cross-chain bridges.

The conclusion offered in this world should be taken with caution, due to research limitations, such as database selection, language biases, and sample size. The review relies exclusively on Scopus and EBSCO and the search was restricted to English-language publications. Given the global nature of quantum research, particularly in China and Europe, this exclusion likely omits potentially relevant contributions in other databases or non-English contributions. Additionally, the final dataset of 27 papers is a small sample set. The findings reflect the core academic consensus but may not capture fringe or emerging theories. Still, the findings are illustrative of the state of the art in academic research and the considerations of PQC in blockchain.

7 Bibliography

Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2018). Quantum attacks on Bitcoin, and how to protect against them. *Ledger*, *3*, 68–90. https://doi.org/10.5195/ledger.2018.127

Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Kelsey, J., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2022). *Status report on the third round of the NIST post-quantum cryptography standardization process*. National Institute of Standards and Technology.

Alfaw, A., Elmedany, W., & Sharif, M. S. (2022). Blockchain Vulnerabilities and Recent Security Challenges: A Review Paper. *2022 International Conference on Data Analytics for Business and Industry, ICDABI 2022*, 780–786. https://doi.org/10.1109/ICDABI56818.2022.10041611

Alghamdi, S., & Almuhammadi, S. (2021). The Future of Cryptocurrency Blockchains in the Quantum Era. *Proceedings - 2021 IEEE International Conference on Blockchain, Blockchain 2021*, 544–551. https://doi.org/10.1109/Blockchain53845.2021.00082

Allende, M., López León, D., Cerón, S., Leal, A., Pareja, A., Pacheco, M., Arias, D., Pontiveros Barrios, B., Culman, M., Villalba, D., Sandoval, D., Montenegro, E., Murcia, D., Levi, A., Ramirez, A., Rendon, A., & Byrne, D. (2023). Quantum-resistance in blockchain networks. *Scientific Reports*, *13*(1), 5664. https://doi.org/10.1038/s41598-023-32701-6

Banerjee, B., Jani, A., & Shah, N. (2021). Asymmetric Confidentiality in Blockchain Embedded Smart Grids in Galois Field. *Frontiers in Blockchain*, *4*. https://doi.org/10.3389/fbloc.2021.770074

Begimbayeva, Y., Zhaxalykov, T., Akhtanov, A., Pashkevich, R., Ussatova, O., & Arshidinova, M. (2025). DESIGN OF A QKD PROTOCOL RESISTANT TO INSIDER ATTACKS IN FULLY CONNECTED DECENTRALIZED NETWORKS. *Eastern-European Journal of Enterprise Technologies*, *4*(9–136), 43–50. https://doi.org/10.15587/1729-4061.2025.337992

Dahhak, H., Afifi, N., & Hilal, I. (2024). Security Analysis of Classical and Post-Quantum Blockchains. *Journal of Computer Information Systems*. https://doi.org/10.1080/08874417.2024.2433263

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, *133*, 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

Egger, D. J., Gambella, C., Marecek, J., McFaddin, S., Mevissen, M., Raymond, R., Simonetto, A., Woerner, S., & Yndurain, E. (2020). Quantum computing for finance: State-of-the-art and future prospects. *IEEE Transactions on Quantum Engineering*, *1*, 1–24. https://doi.org/10.1109/TQE.2020.3030314

Esgin, M. F., Kuchta, V., Sakzad, A., Steinfeld, R., Zhang, Z., Sun, S., & Chu, S. (2021). *Practical post-quantum few-time verifiable random function with applications to Algorand*. 560–578. https://doi.org/10.1007/978-3-662-64322-8_27

Fernández-Caramés, T. M. (2019). From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. *IEEE Internet of Things Journal*, *7*(7), 6457–6480. https://doi.org/10.1109/JIOT.2019.2958788

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access*, *8*, 21091–21116. https://doi.org/10.1109/ACCESS.2020.2968985

Golchha, R., Lachure, J., & Doriya, R. (2023). Fog Enabled Cyber Physical System Authentication and Data Security using Lattice and Quantum AES Cryptography.

International Journal of Computing and Digital Systems, *13*(1), 267–275. https://doi.org/10.12785/ijcds/130122

Grover, L. K. (1996). *A fast quantum mechanical algorithm for database search*. 212–219. https://doi.org/10.1145/237814.237866

Gurung, D., Pokhrel, S. R., & Li, G. (2024). Performance analysis and evaluation of postquantum secure blockchained federated learning. *Computer Networks*, *255*. https://doi.org/10.1016/j.comnet.2024.110849

Holcomb, A., Pereira, G., Das, B., & Mosca, M. (2021, May 3). PQFabric: A permissioned blockchain secure from both classical and quantum attacks. *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2021*. https://doi.org/10.1109/ICBC51069.2021.9461070

Hu, J. W. (2025). A Prototype for Post-Quantum Cryptographic Migration in Hyperledger Fabric. *2025 IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2025*. https://doi.org/10.1109/ICBC64466.2025.11114457

Jency Rubia, J., Babitha Lincy, R., Nithila, E. E., Sherin Shibi, C., & Rosi, A. (2024). A Survey about Post Quantum Cryptography Methods. *EAI Endorsed Transactions on Internet of Things*, *10*. https://doi.org/10.4108/eetiot.5099

Jin, S. (2024). The paradigm logic of blockchain governance. *Technology in Society*, *78*. https://doi.org/10.1016/j.techsoc.2024.102681

Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V, Lvovsky, A. I., & Fedorov, A. K. (2018). Quantum-secured blockchain. *Quantum Science and Technology*, *3*(3), 035004. https://doi.org/10.1088/2058-9565/aabc6b

Kumar, A., Shrimal, V. M., & Rubbina, R. (2025). Analysing security and efficiency in a quantum resistant decentralised E-voting system using blockchain, homomorphic encryption and zero knowledge proofs. *2nd International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering, RMKMATE 2025*. https://doi.org/10.1109/RMKMATE64874.2025.11042466

Liu, F., He, S., Li, Z., & Li, Z. (2023). An overview of blockchain efficient interaction technologies. In *Frontiers in Blockchain* (Vol. 6). Frontiers Media SA. https://doi.org/10.3389/fbloc.2023.996070

Liu, H., Wang, Z., & Knottenbelt, W. (2025). Towards Building Post-Quantum Secure Ethereum. *2025 IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2025*. https://doi.org/10.1109/ICBC64466.2025.11114696

Liu, S., Rao, S., Wang, X. A., Tian, K., & Wang, Y. (2025). PQ-BCDA: A post-quantum blockchain based cross-domain authentication scheme for Internet of Things. *Internet of Things (The Netherlands)*, *33*. https://doi.org/10.1016/j.iot.2025.101737

Mosteanu, N. R., & Faccia, A. (2021). Fintech frontiers in quantum computing, fractals, and blockchain distributed ledger: Paradigm shifts and open innovation. *Journal of Open Innovation: Technology, Market, and Complexity*, *7*(1), 1–19. https://doi.org/10.3390/joitmc7010019

Naik, A. S., Yeniaras, E., Hellstern, G., Prasad, G., & Vishwakarma, S. K. L. P. (2025). From portfolio optimization to quantum blockchain and security: a systematic review of quantum computing in finance. In *Financial Innovation* (Vol. 11, Issue 1). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1186/s40854-025-00751-6

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

Preethi, Ulla, M. M., Sapna, R., & Mohan, K. G. (2023). Implementing Post-Quantum Cryptography Algorithm in Blockchain. *2023 International Conference on New Frontiers in Communication, Automation, Management and Security, ICCAMS 2023*. https://doi.org/10.1109/ICCAMS60113.2023.10525729

Preskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum*, *2*, 79. https://doi.org/10.22331/q-2018-08-06-79

Rad, F. F. (2021). From Far East to Baltic Sea: Impact of Quantum Computers on Supply Chain Users of Blockchain. *International Journal of Enterprise Information Systems*, *17*(4), 85–97. https://doi.org/10.4018/IJEIS.2021100105

Rajan, D., & Visser, M. (2019). Quantum blockchain using entanglement in time. *Quantum Reports*, *1*(1), 3–11. https://doi.org/10.3390/quantum1010002

Rehman, M. H. U., Salah, K., Damiani, E., & Svetinovic, D. (2020). Trust in Blockchain Cryptocurrency Ecosystem. *IEEE Transactions on Engineering Management*, *67*(4), 1196–1212. https://doi.org/10.1109/TEM.2019.2948861

Rivest R, S. A. A. L. (1978). *A method for obtaining digital signatures, public-key cryptosystems*.

Seol, J., & Kim, J. (2023). Quantum threat and dependability of quantum-safe blockchain-based distributed control systems and network. *Issues in Information Systems*, *24*(3), 144–158. https://doi.org/10.48009/3_iis_2023_113

Shafeeq, S., Zeadally, S., Alam, M., & Khan, A. (2020). Curbing Address Reuse in the IOTA Distributed Ledger: A Cuckoo-Filter-Based Approach. *IEEE Transactions on Engineering Management*, *67*(4), 1244–1255. https://doi.org/10.1109/TEM.2019.2922710

Shahid, F., & Khan, A. (2020). Smart Digital Signatures (SDS): A post-quantum digital signature scheme for distributed ledgers. *Future Generation Computer Systems*, *111*, 241–253. https://doi.org/10.1016/j.future.2020.04.042

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, *26*(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Weinberg, A. I., Petratos, P., & Faccia, A. (2025). Will Central Bank Digital Currencies (CBDC) and blockchain cryptocurrencies coexist in the post quantum era? *Discover Analytics*, *3*(1). https://doi.org/10.1007/s44257-025-00034-5

Yi, H. (2023). An Efficient E-Voting System for Business Intelligence Innovation Based on Blockchain. *Journal of the Knowledge Economy*. https://doi.org/10.1007/s13132-023-01560-x

Yi, H., Li, Y., Wang, M., Yan, Z., & Nie, Z. (2021). An Efficient Blockchain Consensus Algorithm Based on Post-Quantum Threshold Signature. *Big Data Research*, *26*. https://doi.org/10.1016/j.bdr.2021.100268

Yin, W., Wen, Q., Li, W., Zhang, H., & Jin, Z. (2018). An anti-quantum transaction authentication approach in blockchain. *IEEE Access*, *6*, 5393–5401. https://doi.org/10.1109/ACCESS.2017.2788411

Yoon, J., Alkhudary, R., Talluri, S., & Fenies, P. (2025). Risk Management and Macroeconomic Disruptions in Supply Chains: The Role of Blockchain, Digital Twins, Generative AI, and Quantum Computing. *IEEE Transactions on Engineering Management*, *72*, 2995–3009. https://doi.org/10.1109/TEM.2025.3585433

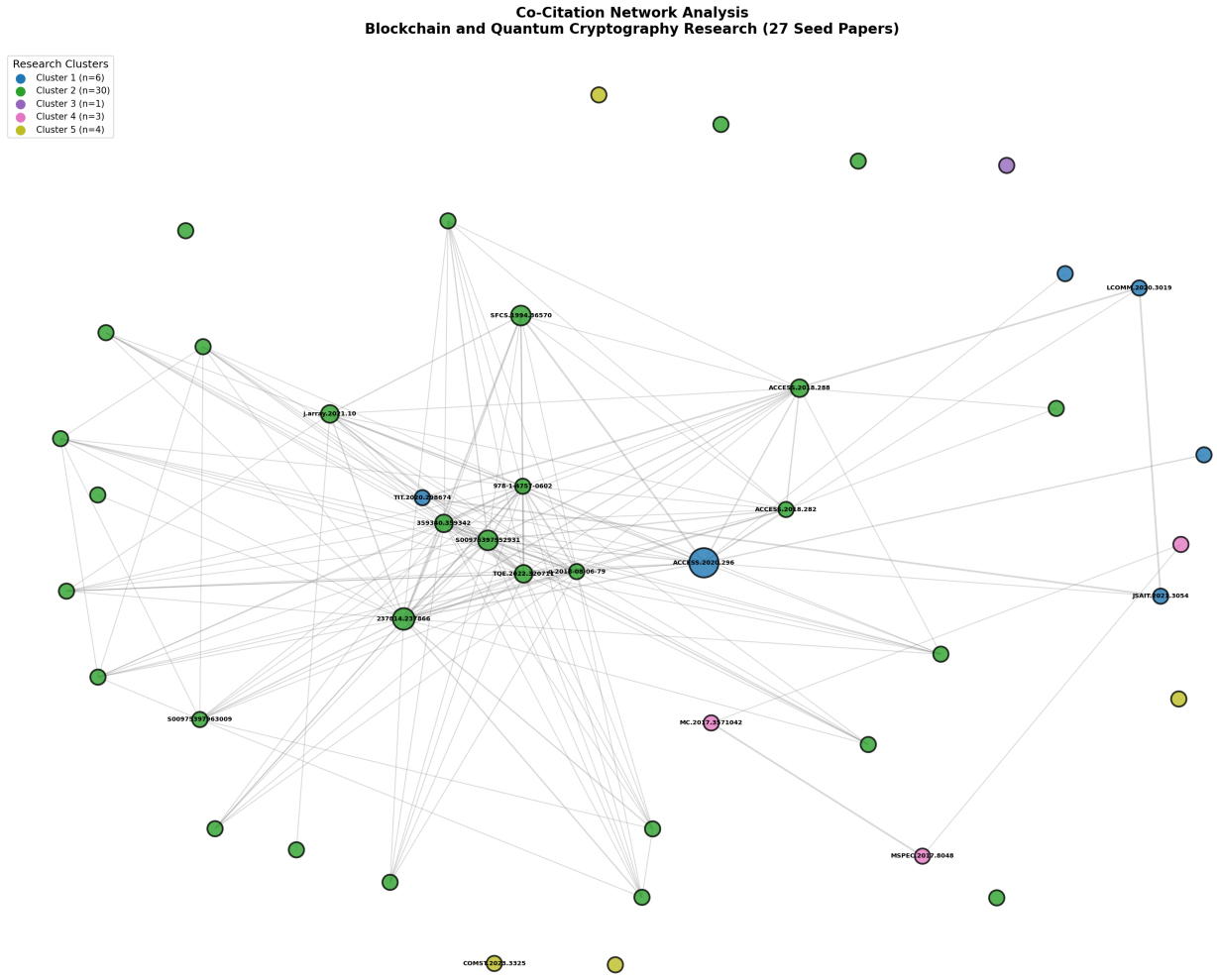
Appendix

Appendix 1 - Paper ID's for SLR

Paper ID	Title
1	Trust in Blockchain Cryptocurrency Ecosystem (Rehman et al., 2020)
2	Fintech Frontiers in Quantum Computing, Fractals, and Blockchain Distributed Ledger: Paradigm Shifts and Open Innovation (Mosteanu & Faccia, 2021)
3	Curbing Address Reuse in the IOTA Distributed Ledger- A Cuckoo-Filter-Based Approach (Shafeeq et al., 2020)
4	An Efficient Blockchain Consensus Algorithm Based on Post-Quantum Threshold Signature (Yi et al., 2021)
5	PQFabric- A Permissioned Blockchain Secure from Both Classical and Quantum Attacks (Holcomb et al., 2021)
6	An overview of blockchain efficient interaction technologies (F. Liu et al., 2023)
7	A Survey about Post Quantum Cryptography Methods (Jency Rubia et al., 2024)
8	The Future of Cryptocurrency Blockchains in the Quantum Era (Alghamdi & Almuhammadi, 2021)
9	An Efficient E-Voting System for Business Intelligence Innovation Based on Blockchain(Yi, 2023)
10	From portfolio optimization to quantum blockchain and security- a systematic review of quantum computing in finance(Naik et al., 2025)
11	Blockchain Vulnerabilities and Recent Security Challenges- A Review Paper(Alfaw et al., 2022)
12	Asymmetric Confidentiality in Blockchain Embedded Smart Grids in Galois Field(Banerjee et al., 2021)
13	From Far East to Baltic Sea- Impact of Quantum Computers on Supply Chain Users of Blockchain (Rad, 2021)
14	Fog Enabled Cyber Physical System Authentication and Data Security using Lattice and Quantum AES Cryptography (Golchha et al., 2023)
15	Risk Management and Macroeconomic Disruptions in Supply Chains- The Role of Blockchain, Digital Twins, Generative AI, and Quantum Computing(Yoon et al., 2025)
16	Implementing Post-Quantum Cryptography Algorithm in Blockchain(Preethi et al., 2023)
17	PQ-BCDA- A post-quantum blockchain based cross-domain authentication scheme for Internet of Things(S. Liu et al., 2025)
18	Design of a QKD protocol resistant to insider attacks in fully connected decentralized networks(Begimbayeva et al., 2025)
19	Analysing security and efficiency in a quantum resistant decentralised E-voting system using blockchain, homomorphic encryption and zero knowledge proofs(Kumar et al., 2025)
20	Towards Building Post-Quantum Secure Ethereum(H. Liu et al., 2025)
21	A Prototype for Post-Quantum Cryptographic Migration in Hyperledger Fabric(Hu, 2025)
22	The paradigm logic of blockchain governance(Jin, 2024)

23	Quantum threat and dependability of quantum-safe blockchain- based distribu(Seol & Kim, 2023)s and network(Seol & Kim, 2023)
24	Performance analysis and evaluation of postquantum secure blockchained federated learning (Gurung et al., 2024)
25	Security Analysis of Classical and Post-Quantum Blockchains (Dahhak et al., 2024)
26	Smart Digital Signatures (SDS)- A post-quantum digital signature scheme for distributed ledgers (Shahid & Khan, 2020)
27	Will Central Bank Digital Currencies (CBDC) and blockchain cryptocurrencies coexist in the post quantum era? (Weinberg et al., 2025)

Appendix 2 - Co-citation network



Appendix 3 - Statement of GenAI Use

I hereby certify that I adhered to the SBE guidelines on the use of GenAI tools such as ChatGPT in the master thesis. Below I document how and for what purposes I used GenAI. During the preparation of this work, I used GenAI for the following purposes:

- Search engine: EBSCO, SCOPUS
- Ideation helper: Elicit AI (for structuring research questions and refining frameworks)
- Text summarizer: Gemini & Elicit AI (for summarizing complex academic papers and synthesize key points)
- Code writer: SciSpace.com (For creating the python code needed to analyze papers
- Explanation provider: Gemini (for clarifying papers)
- Language assistant: Gemini (for paraphrasing and rephrasing sentences for the ease of understanding and academic tone)

After using any tool, I reviewed, quality-checked, and edited the content as needed and take full responsibility for the content of the thesis.

Place: Lisbon, Portugal
Date: 27-11-2025
First and last name: Florine Shifra Elskamp, Student ID: 68345
Study program: Impact Entrepreneurship & Innovation

Signature: .....