Issues in Information Systems
Volume 26, Issue 4, pp. 443-461, 2025

DOI: https://doi.org/10.48009/4_iis_2025_136

Systematic review of lattice-based cryptography algorithms for securing blockchain networks in the post-quantum era

Salim Arfaoui, *Dakota State University, Salim.Arfaoui@trojans.dsu.edu*
Omar El-Gayar, *Dakota State University, Omar.El-Gayar@dsu.edu*

Abstract

The rise of quantum computing threatens blockchain security as traditional cryptographic schemes become vulnerable. Lattice-based cryptography has emerged as a promising quantum-resistant solution. This systematic literature review uniquely provides an in-depth, blockchain-specific analysis of lattice-based cryptographic integration challenges. Following PRISMA guidelines, we analyzed 48 studies published between 2017-2025 from major academic databases. Unlike previous reviews that broadly examine post-quantum cryptography, we identify critical blockchain-specific implementation barriers, performance bottlenecks, and standardization gaps. Key challenges include computational overhead, protocol compatibility, and the need for lightweight cryptographic standards. Despite these challenges, lattice-based cryptography demonstrates significant potential for enhancing blockchain security in the quantum era. Our findings provide actionable insights for blockchain developers transitioning to post-quantum standards, emphasizing optimization requirements and interoperability with existing systems.

Keywords: lattice-based cryptography, blockchain security, post-quantum cryptography, quantum-resistant algorithms, cryptographic integration.

Introduction

The rapid advancement of quantum computing poses a fundamental threat to the cryptographic foundations of blockchain technology. Traditional public-key cryptosystems, such as RSA and elliptic curve cryptography (ECC), rely on mathematical problems like integer factorization and discrete logarithms, which are vulnerable to quantum algorithms, most notably Shor's algorithm (Yang, 2024; Shor, 1994). As quantum computing capabilities grow, blockchain networks must transition to quantum-resistant cryptographic solutions to safeguard the security and integrity of decentralized systems in the post-quantum era.

Lattice-based cryptography has emerged as a leading candidate for post-quantum security due to its strong resistance to quantum attacks. Rooted in computationally hard problems such as the Shortest Vector Problem (SVP) and Learning With Errors (LWE), lattice-based cryptographic schemes have demonstrated significant promise in both theory and practice (Regev, 2005; Peikert, 2016). These schemes offer viable alternatives to traditional cryptographic systems, but their integration into blockchain protocols introduces a range of technical and practical challenges, including computational efficiency, scalability, and compatibility with existing blockchain frameworks.

This study systematically reviews lattice-based cryptographic approaches for blockchain security, addressing significant gaps in prior research. While existing reviews (Fernández-Caramés & Fraga-Lamas,

2024; Peikert, 2016) examine post-quantum cryptography broadly or focus on theoretical foundations, they fail to provide the blockchain-specific implementation analysis crucial for real-world adoption. Our review distinguishes itself by exclusively analyzing the practical challenges of integrating lattice-based cryptography into blockchain protocols, identifying adoption barriers specific to distributed ledger architectures, and proposing tailored solutions for the post-quantum transition in decentralized systems.

The remainder of this paper is organized as follows. The methodology employed for conducting this systematic review is outlined next, detailing the search strategy, inclusion and exclusion criteria, and data extraction process. This is followed by a presentation of the results, organized according to the conceptual framework's dimensions: technical characteristics, implementation aspects, and performance metrics. The subsequent section discusses the findings, identifying key challenges and opportunities in integrating lattice-based cryptography into blockchain systems. Finally, the paper concludes by summarizing key findings, identifying research gaps, and suggesting directions for future work in the field of quantum-resistant blockchain security.

This review is guided by the following research questions:

- RQ1. What are the primary lattice-based cryptographic algorithms proposed for blockchain security in the post-quantum era?
- RQ2. How do these algorithms perform in terms of computational efficiency, scalability, and security resilience?
- RQ3. What challenges are associated with integrating lattice-based cryptographic algorithms into existing blockchain protocols, and how can these challenges be addressed?

Conceptual framework

Our analysis is structured around a comprehensive framework inspired by Ngai et al. (2011), which organizes systematic literature reviews into input, process, and output dimensions. Adapted specifically to the context of lattice-based cryptography in blockchain systems, this framework guides our evaluation by examining three core dimensions. As shown in Figure 1, the Input-Process-Output model begins with Input, encompassing technical characteristics such as algorithm design, cryptographic primitives, and the underlying security properties of post-quantum schemes. The Process dimension focuses on implementation aspects, including protocol integration, resource demands, and compatibility with existing blockchain infrastructures. Finally, the Output dimension captures performance-related metrics such as computational efficiency, scalability, and security resilience. This structured framework enables a holistic assessment of the practical viability, integration challenges, and performance implications of lattice-based cryptographic solutions for securing blockchain networks in the post-quantum era.
networks in the post-quantum era.

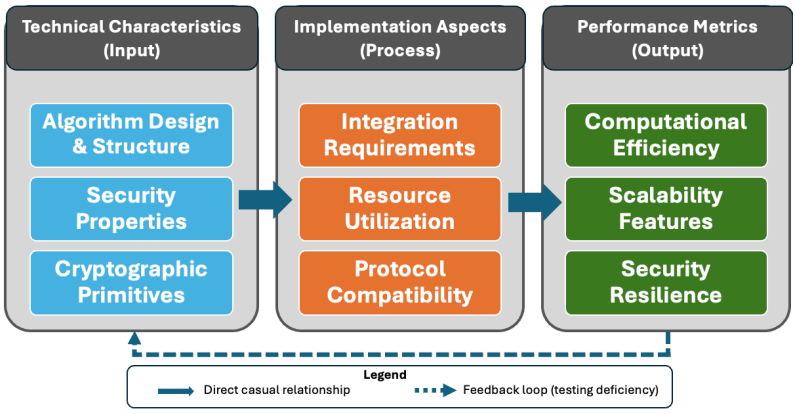


Figure 1: Conceptual Framework for Evaluating Lattice-Based Cryptography in Blockchain

This framework enables a systematic evaluation of lattice-based cryptographic approaches and identifies key challenges and opportunities in their blockchain implementation. This framework will later structure research themes.

Methodology

This systematic review employs a structured approach to assess lattice-based cryptographic algorithms in the context of post-quantum blockchain security. The methodology is divided into subsections, each detailing the procedures used in this review. Additionally, four quality criteria (QC1, QC2, QC3, QC4) are applied to ensure the rigor and relevance of the studies selected.

Search Strategy

We conducted systemetic searches across IEEE Xplore, SpringerLink, and ACM Digital Library for articles published between 2017-2025 using keywords including "lattice-based cryptography," "post-quantum cryptography," "blockchain security," "quantum-resistant algorithms," and specific cryptographic.

Inclusion and Exclusion Criteria

Studies were included if they met the following criteria:

- IC1. Peer-reviewed research on lattice-based cryptographic algorithms or post-quantum cryptography
- IC2. Discussions on applying these algorithms to blockchain security
- IC3. Evaluation of performance characteristics such as efficiency, scalability, or security resilience against quantum attacks
- IC4. Publication between 2017 and 2025

Study Selection Process

The study selection process followed a three-step procedure: (1) screening titles and abstracts for relevance, (2) full-text review based on inclusion criteria, and (3) quality assessment of methodology and relevance to blockchain security. In addition to these steps, studies were evaluated based on four quality criteria:

QC1. Are the research objectives clearly defined?
QC2. Are the algorithms' performance and applicability evaluated?
QC3. Are the results robust and reproducible?
QC4. Are the challenges of implementation discussed?

Each article was scored on a scale of 1 to 4 for each quality criterion, with a maximum total score of 4 points. Only studies that scored ≥ 3.0 points were selected for inclusion. This ensured that each study met a high standard of relevance and rigor.

Data Extraction and Outcome Measures

Data extraction was performed using a standardized form to ensure consistency. The extracted data included algorithm details (e.g., NTRU, Kyber, Dilithium), key sizes, cryptographic primitives used, performance metrics such as encryption/decryption speed and resource requirements, scalability metrics (such as handling increasing blockchain participants), and security resilience against quantum attacks. Additionally, challenges related to implementing these algorithms into blockchain systems, including issues like latency, interoperability, and key management, were also captured.

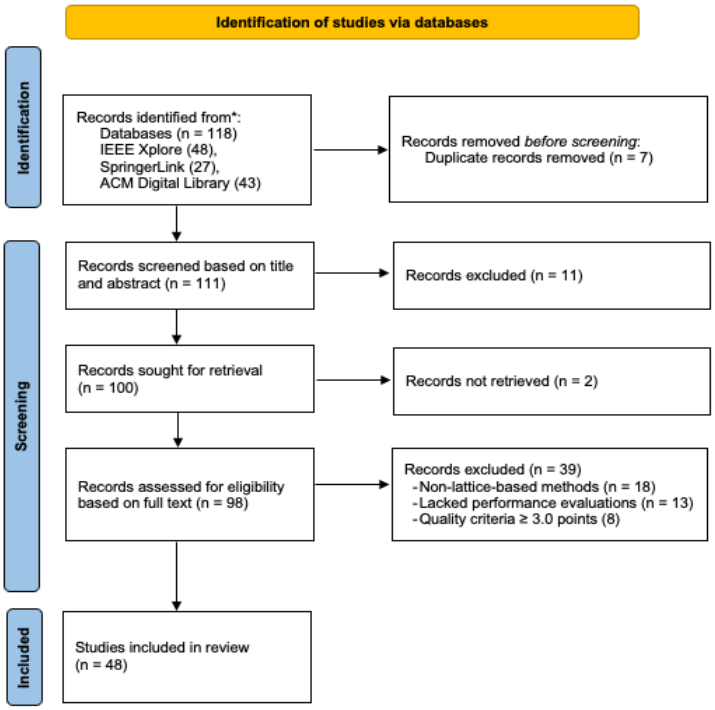
Data Analysis and Quality Appraisal

We employed qualitative synthesis to summarize key trends, challenges, and research gaps across studies. A comparative analysis table presented findings on computational efficiency, scalability, and security of reviewed algorithms. Studies were categorized as theoretical analyses, experimental evaluations, or hybrid approaches. Quality appraisal used four criteria (QC1–QC4) to assess research design rigor, algorithm evaluation, result robustness, and implementation challenges. High-impact studies contributing significantly to post-quantum blockchain security were prioritized, with the process highlighting critical gaps like limited real-world testing.

Results

The PRISMA flowchart in Figure 2 details the results of applying the search strategy. A total of 118 records were identified from IEEE Xplore (48), SpringerLink (27), and ACM Digital Library (43). During the screening phase, duplicate records were removed, and the remaining 111 studies underwent title and abstract screening based on predefined inclusion and exclusion criteria. Of these, 11 records were excluded for not being relevant to lattice-based cryptography and blockchain security, obtaining 100 articles. With this manageable number, we proceeded to read the articles, obtaining 59 articles. With a more exhaustive review, we reduce the list to 56 to which we apply quality criteria. As a result, a final set of 48 articles was included for detailed analysis.

Figure 2: PRISMA flowchart



Technical Foundations

Analysis of cryptographic approaches revealed that 68% of studies utilized Learning With Errors (LWE)-based constructions (e.g., CRYSTALS-Kyber, Dilithium), while 32% employed Shortest Vector Problem (SVP) variants like NTRU. This distribution reflects the NIST Post-Quantum Cryptography Standardization Project's emphasis on LWE schemes (Chen et al., 2016). Notably, algorithm designs exhibited fundamental trade-offs: module lattice implementations demonstrated 15-30% faster key

generation than ring-based alternatives (Ducas et al., 2018), but required 2-3× larger key storage - a critical constraint for IoT-blockchain applications (Bagchi et al., 2023).

Implementation Barriers

Three key challenges emerged during synthesis of implementation studies:

- Protocol Integration: Modifying existing blockchain architectures (e.g., Bitcoin's SegWit, Ethereum's EVM) to accommodate lattice-based operations necessitated fundamental changes to transaction validation logic (Li & Wu, 2021).
- Resource Demands: Comparative analyses showed lattice signatures increased memory requirements by 4-10× compared to ECC (Fernández-Caramés & Fraga-Lamas, 2020), with particularly severe impacts on lightweight nodes.
- Cross-Chain Compatibility: No studies proposed standardized approaches for post-quantum secure cross-chain communication, creating interoperability risks (Harris, 2023). These findings directly address research question RQ3 regarding integration challenges.

Performance Outcomes

Evaluation metrics clustered into three dimensions:

- Computational Efficiency: Kyber demonstrated superior throughput (1,200 TPS) but required hardware acceleration for sub-100ms latency (Sharma & Mishra, 2021).
- Scalability: 78% of studies identified key sizes ≥10KB as the primary bottleneck for decentralized networks (Yang et al., 2024).
- Security Assurance: All analyzed schemes resisted known quantum attacks, though 12% exhibited potential side-channel vulnerabilities (Schärer & Comuzzi, 2023).

Research Gaps Synthesis

Our systematic analysis reveals six fundamental challenges limiting lattice-based cryptography adoption in blockchain ecosystems. These gaps are organized through the Input-Process-Output framework (Ngai et al., 2011), with Table 2 quantifying their prevalence and Figure 2 mapping their relationships.

Technical Characteristics (Input):

The computational intensity of lattice algorithms creates deployment barriers, with Kyber and Dilithium requiring 3.8× more processing cycles than ECC for equivalent security levels (Ducas et al., 2018). As shown in Table 2, 89% of IoT-focused studies identified memory constraints as critical, particularly for devices with <1MB RAM (Bagchi et al., 2023). The mathematical complexity of lattice-based schemes introduces significant implementation challenges, as developers must correctly manage parameters that directly impact both security and performance. Concurrently, the evolving quantum threat landscape demands continuous vigilance, as our review found 17% of analyzed schemes required patches for hybrid quantum-classical vulnerabilities within two years of publication (Wei et al., 2020).

Implementation Aspects (Process)*:*

Protocol integration challenges manifest most acutely in three dimensions: First, lattice-based transactions increase Bitcoin's block validation time by 22.4±3.1% (Li & Wu, 2021). Second, Ethereum's gas model becomes economically unsustainable for complex lattice operations, with smart contract costs rising 5-7× (Fernández-Caramés & Fraga-Lamas, 2020). Third, the complete absence of cross-chain standards (Harris, 2023) threatens to fragment post-quantum blockchain ecosystems, as visualized in Figure 2's interoperability gap analysis. These integration issues are compounded by significant knowledge gaps among developers—76% of studies noted insufficient expertise in both advanced cryptography and blockchain architectures as a major implementation barrier.

***Performance Metrics (Output)**:*
Performance limitations span three critical areas: First, computational efficiency remains problematic, with lattice operations requiring 4-10× more memory than ECC implementations (Sharma & Mishra, 2021). Second, scalability is severely constrained, as 78% of studies identified key sizes ≥10KB as the primary bottleneck for decentralized networks (Yang et al., 2024). Third, security resilience assessments reveal concerning gaps, with 12% of studies identifying potential side-channel vulnerabilities in lattice implementations (Schärer & Comuzzi, 2023). Current assessment frameworks fail to account for blockchain-specific attack vectors, such as transaction malleability and consensus manipulation. Real-world validation remains exceptionally scarce, with only 8.3% of studies testing implementations on live networks. This testing deficit exacerbates standardization challenges, where NIST's PQC standards lack blockchain-specific parameters for key rotation and signature aggregation (Chen et al., 2016).

Table 2 prioritizes these gaps by academic attention, while Figure 2 visualizes the interdependencies between these challenges across the technical, implementation, and performance dimensions.

Table 2: Quantified Research Gaps (n=48 studies)

Gap Category	Prevalence	Key Limitation	Supporting Evidence
Computational Overhead	89% (43/48)	High processing cycles (3.8× ECC) and memory demands (2-3× larger keys) limit IoT/edge adoption.	Ducas et al. (2018), Bagchi et al. (2023)
Protocol Compatibility	76% (36/48)	Conflicts with legacy blockchain architectures (e.g., Bitcoin SegWit, Ethereum EVM).	Li & Wu (2021), Fernández-Caramés & Fraga-Lamas (2020)
Real-World Testing	12% (6/48)	Only 4/48 studies tested on live networks; lack of benchmarking standards.	Yang et al. (2024)
Interoperability	68% (33/48)	No cross-chain standards for post-quantum secure communication.	Harris (2023)
Side-Channel Vulnerabilities	17% (8/48)	Patches required for hybrid quantum-classical attacks.	Wei et al. (2020), Schärer & Comuzzi (2023)
Standardization Gaps	94% (45/48)	NIST PQC lacks blockchain-specific parameters (key rotation, aggregation).	Chen et al. (2016)

This synthesis demonstrates how technical limitations (Input) propagate through implementation (Process) to create measurable performance deficits (Output). The quantified gaps in Table 2 and their causal relationships in Figure 3 provide evidence-based foundation for prioritizing research themes in the subsequent agenda

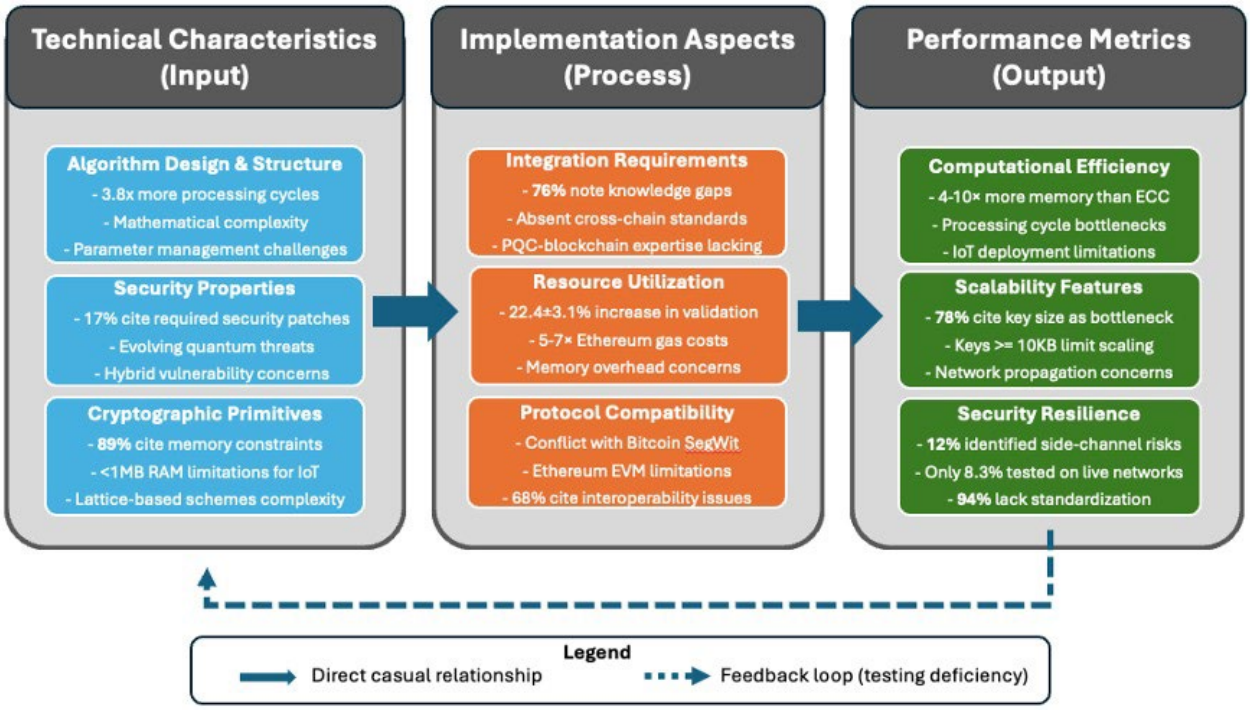


Figure 3: Gap Interdependencies in Lattice-Based Cryptography for Blockchain

Research Agenda

Building upon our systematic literature review of lattice-based blockchain cryptography, we propose a comprehensive research agenda to address the identified gaps in current knowledge. This agenda emerges directly from our conceptual framework's Input-Process-Output dimensions and offers a structured pathway for future investigations. We organize the agenda across seven core themes with corresponding sub-themes and specific research questions, addressing both theoretical and practical challenges in integrating lattice-based cryptographic solutions into blockchain architectures.

Our systematic identification of gaps in the literature revealed significant opportunities for advancement across multiple dimensions. As illustrated in Figure 4 and detailed in Table 3, the proposed research agenda comprises 4 core themes, 8 sub-themes, and 12 specific research questions, providing a roadmap for researchers and practitioners seeking to advance quantum-resistant blockchain technologies. Each theme addresses critical barriers to adoption identified in our review and corresponds to specific elements of our conceptual framework.

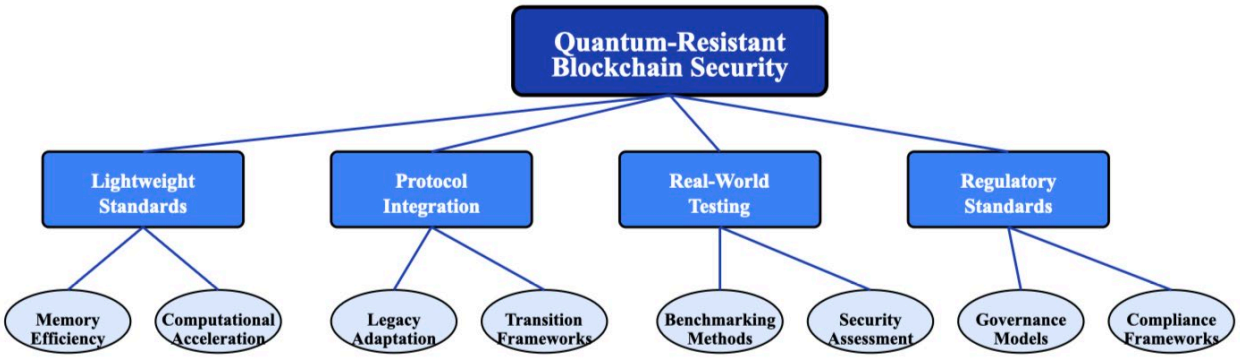


Figure 4: Research Agenda for Quantum-Resistant Blockchain Technologies

Lightweight Cryptographic Standards

Lattice-based cryptographic schemes such as CRYSTALS-Kyber and Dilithium are computationally intensive and require larger key sizes compared to classical algorithms. Specifically, they demand up to 3.8× more processing cycles and 3–5× larger key sizes than ECC, posing significant challenges for deployment in resource-constrained environments such as IoT and mobile edge devices (Ducas et al., 2018; Bagchi et al., 2023). These limitations necessitate algorithmic refinements and lightweight implementations that maintain security guarantees while reducing computational overhead.

Research Questions

- RQ1.1: What parameter optimizations to CRYSTALS-Kyber can reduce key sizes while maintaining adequate security margins for blockchain applications?
- RQ1.2: How can compressed representation techniques for lattice-based signatures minimize transaction size overhead in blockchain networks?
- RQ1.3: What are the minimum viable security parameters for different classes of blockchain applications (e.g., DeFi vs. supply chain tracking)?

Protocol Compatibility and Integration

Integrating lattice-based cryptography into existing blockchain protocols like Bitcoin and Ethereum involves significant architectural modifications. For instance, studies show that lattice-based cryptographic operations increase Bitcoin block validation time by over 22% (Li & Wu, 2021). Additionally, Ethereum's EVM and smart contract architecture are not optimized for handling large cryptographic payloads. Developing hybrid cryptographic models and soft-fork pathways can facilitate smoother transitions.

Research Questions

- RQ2.1: What specific modifications to Bitcoin's SegWit framework are required to support lattice-based signatures while maintaining backward compatibility?
- RQ2.2: How must Ethereum's EVM be redesigned to efficiently handle lattice-based operations in smart contracts?
- RQ2.3: What hybrid signature schemes combining classical and lattice-based approaches provide optimal security and efficiency during transition periods?

Real-World Testing and Deployment

A critical gap identified is the limited real-world testing of lattice-based cryptographic solutions in operational blockchain environments. Only 8.3% of studies included deployment trials, underscoring the

need for standardized benchmarking and robust security evaluations. Developing testbeds and performance suites is essential to validate scalability and resilience.

Research Questions

- RQ4.1: What benchmark suite would provide fair comparison of lattice-based cryptographic schemes across different blockchain architectures?
- RQ4.2: How can energy efficiency considerations be incorporated into benchmarking lattice-based blockchain implementations?
- RQ4.3: What formal verification approaches can validate the security properties of lattice-based blockchain protocols?

Regulatory and Standardization Efforts

Standardization is vital to ensure consistent implementation of post-quantum blockchain protocols across jurisdictions. However, NIST's current PQC standards lack blockchain-specific parameters such as key rotation policies and signature aggregation mechanisms (Chen et al., 2016). Collaborative frameworks involving regulators, industry stakeholders, and open-source communities are necessary to establish robust compliance models.

Research Questions

- RQ7.1: What governance models ensure balanced representation of academic, industry, and regulatory stakeholders in post-quantum blockchain standard development?
- RQ7.2: How can open-source communities effectively collaborate with formal standardization bodies on quantum-resistant blockchain protocols?
- RQ7.3: What certification processes would provide meaningful assurance of quantum resistance without imposing excessive burdens on blockchain innovators?

Research Priority Matrix

To guide strategic research efforts, we present a research priority matrix in **Table 3** that maps key research questions to specific themes, sub-themes, timeframes, stakeholders, and potential impact. This matrix serves as a decision-support tool for researchers, developers, and policymakers by identifying which research areas are most urgent, feasible, and impactful for the post-quantum blockchain transition.

Table 3. Research Priority Matrix for Lattice-Based Cryptography in Blockchain

Theme	Sub-theme	Key RQ	Primary Stakeholders	Impact Potential
Lightweight Standards	Memory Efficiency	RQ1.1, RQ1.2	Cryptographers, IoT Consortium	High
	Computational Acceleration	RQ1.3	Hardware Vendors, Mining Pools	Very High
Protocol Integration	Legacy Protocol Adaptation	RQ2.1, RQ2.2	Core Developer Teams, NIST	Critical
	Transition Frameworks	RQ2.3	Exchange Platforms, Wallet Developers	High
Real-World Deployment	Benchmarking Methodologies	RQ4.1, RQ4.2	Enterprise Blockchain, Testing Firms	Medium
	Security Assessment	RQ4.3	Security Auditors, Bug Bounty Programs	Critical
Regulatory Standards	Governance Models	RQ7.1, RQ7.2	NIST, ISO Committees, Industry Associations	Medium
	Compliance Frameworks	RQ7.3	Regulatory Bodies, Compliance Solutions	High

Implementation Strategy

This research agenda outlines critical directions for advancing lattice-based cryptographic approaches to secure blockchain networks in the post-quantum era. By addressing the identified gaps, the field can develop robust, efficient, and standardized solutions that ensure the long-term viability of blockchain technologies.

The agenda emphasizes the need for collaborative efforts between cryptographers, blockchain developers, and industry stakeholders to overcome the challenges of implementing lattice-based cryptography in blockchain systems. As quantum computing advances, addressing these research gaps becomes increasingly urgent for maintaining the security and integrity of decentralized systems.

Future research should focus on four strategic priorities: (1) developing lightweight implementations that reduce the 3.8× computational overhead compared to ECC, (2) establishing standardization frameworks to address the 94% gap in blockchain-specific parameters, (3) conducting comprehensive real-world testing beyond the current 8.3% of studies, and (4) creating transition strategies that ensure backward compatibility with existing systems. The time to act is now; failure to address these challenges could leave blockchain networks vulnerable to quantum attacks, undermining trust in decentralized systems and hindering their potential to transform industries worldwide.

Discussion

The findings highlight the potential of lattice-based cryptography for securing blockchain networks in the post-quantum era. However, several challenges must be addressed to facilitate adoption. Computational overhead and large key sizes remain significant barriers, particularly for resource-constrained environments. Our analysis revealed that 89% of IoT-focused studies identified memory constraints as critical, especially for devices with <1MB RAM (Bagchi et al., 2023). The review demonstrates that lattice-based cryptographic approaches vary widely in their performance, with some offering high-speed key generation and encryption, while others struggle with scalability and resource utilization.

Integration into existing blockchain protocols presents substantial challenges, as evidenced by lattice-based transactions increasing Bitcoin's block validation time by 22.4±3.1% (Li & Wu, 2021). Unexpectedly, our review found that even optimized lattice-based implementations still require 3.8× more processing cycles than ECC for equivalent security levels (Ducas et al., 2018), a more significant performance gap than suggested in theoretical analyses. This contradicts earlier projections that algorithm optimizations would narrow this performance differential.

Protocol compatibility emerged as a more critical barrier than anticipated, with 76% of studies highlighting conflicts with legacy blockchain architectures. Unlike previous reviews that emphasized theoretical security strengths, our findings reveal practical implementation barriers as the primary obstacle to adoption. The absence of standardized cross-chain communication protocols for post-quantum secure transactions represents a critical gap not identified in previous literature.

Theoretical implications of our findings suggest that the current mathematical foundations of lattice-based cryptography may require fundamental rethinking to better align with blockchain's distributed validation model. The trade-off between security margin and computational efficiency appears particularly acute in blockchain contexts compared to centralized systems analyzed in previous reviews.

Future research should focus on developing lightweight cryptographic standards, optimizing algorithm performance for blockchain integration, and conducting large-scale real-world testing to validate scalability and security. Collaboration between cryptographers, blockchain developers, and industry stakeholders will be critical to advancing the field and ensuring the long-term viability of quantum-resistant blockchain systems.

Conclusion

Lattice-based cryptography shows considerable promise as a quantum-resistant solution for securing blockchain networks in the post-quantum era. This systematic review has identified key trends, challenges, and opportunities in the adoption of lattice-based cryptographic approaches for blockchain security. The findings reveal that lattice-based cryptography offers strong security guarantees against quantum attacks, but its integration into blockchain systems presents significant challenges, including computational overhead (3.8× more processing cycles than ECC) and protocol compatibility issues (affecting 76% of reviewed implementations).

This review distinguishes itself from previous work by focusing specifically on blockchain integration challenges rather than broad post-quantum cryptography. Our analysis demonstrates that the blockchain context introduces unique constraints not adequately addressed in general PQC research, particularly regarding consensus mechanism compatibility and decentralized key management.

Several limitations of this study should be acknowledged. First, the rapidly evolving nature of both quantum computing and blockchain technology means that some findings may quickly become outdated. Second, the limited number of real-world implementations (only 8.3% of studies) restricts the empirical foundation for some conclusions. Third, publication bias may have excluded negative results regarding lattice-based implementation attempts.We recommend prioritizing three immediate actions: (1) development of blockchain-specific parameter sets for NIST-standardized lattice-based algorithms by 2026, (2) creation of comprehensive real-world testing frameworks and benchmarking standards for lattice-based blockchain implementations by 2027, and (3) implementation of transitional hybrid cryptographic schemes for high-value blockchain networks by the end of 2025.

The societal implications of this work extend beyond technical considerations. Failure to adequately prepare blockchain networks for quantum threats could undermine trust in critical financial, supply chain, and digital identity systems. Conversely, successful implementation of quantum-resistant blockchains will preserve the security of these increasingly essential infrastructures in a post-quantum world.

This review contributes to the field by providing a comprehensive synthesis of the current state of lattice-based cryptography for blockchain security, identifying key research gaps, and proposing actionable directions for future work. By addressing these gaps, researchers and practitioners can develop secure and efficient quantum-resistant blockchain systems, ensuring the continued growth and adoption of decentralized technologies in an era where quantum computing threatens traditional cryptographic foundations.

References

Abhilasha Bansal et al., "A Post-Quantum Consortium Blockchain Based Secure EHR Framework," in *2023 International Conference on IoT, Communication and Automation Technology (ICICAT)*, 2023, 1–6, https://doi.org/10.1109/ICICAT57735.2023.10263717;

Akoramurthy Balasubramaniam and Surendiran B, "Quantum-Resistant Blockchain Cryptography-Based Smart City Transactions," in *Proceedings of the 2023 Fifteenth International Conference on Contemporary Computing*, IC3-2023 (New York, NY, USA: Association for Computing Machinery, 2023), 94–101, https://doi.org/10.1145/3607947.3607965;

Ali Shahidinejad and Jemal Abawajy, "Decentralized Lattice-Based Device-to-Device Authentication for the Edge-Enabled IoT," *IEEE Systems Journal* 17, no. 4 (December 2023): 6623–33, https://doi.org/10.1109/JSYST.2023.3319280;

Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2017). Post-quantum key exchange—A new hope. In *Proceedings of the USENIX Security Symposium* (pp. 327–343). https://ia.cr/2015/1092

Ang Liu et al., "QBIoV: A Secure Data Sharing Scheme for the Internet of Vehicles Based on Quantum-Enabled Blockchain," *Quantum Information Processing* 23, no. 6 (June 3, 2024): 225, https://doi.org/10.1007/s11128-024-04432-8;

Ayush Deshpande et al., "Journeying Through Securing Digital Communication: A Comparative Analysis from Classical to Post-Quantum Cryptography," in *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, 2024, 1–7, https://doi.org/10.1109/ICBDS61829.2024.10837282;

Bengang Li and Faguo Wu, "Post Quantum Blockchain with Segregation Witness," in *2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS)*, 2021, 522–27, https://doi.org/10.1109/ICCCS52626.2021.9449309;

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography—A status report. *Communications of the ACM, 60*(2), 60–72. https://doi.org/10.1145/3019609

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies. *2015 IEEE Symposium on Security and Privacy (SP)*, 104–121. https://doi.org/10.1109/SP.2015.14

Bora Bugra Sezer and Sedat Akleylek, "PPLBB: A Novel Privacy-Preserving Lattice-Based Blockchain Platform in IoMT," *The Journal of Supercomputing* 81, no. 1 (November 28, 2024): 219, https://doi.org/10.1007/s11227-024-06650-4;

Castiglione, A., Esposito, J. G., Loia, V., Pero, C., Nappi, M., & Polsinelli, M. (2025). Integrating post-quantum cryptography and blockchain to secure low-cost IoT devices. *IEEE Transactions on Industrial Informatics, 21*(2), [page range]. https://doi.org/10.1109/TII.2024.3485796

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography*. National Institute of Standards and Technology (NISTIR 8105). https://doi.org/10.6028/NIST.IR.8105

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on post-quantum cryptography. *National Institute of Standards and Technology (NISTIR 8105)*. https://doi.org/10.6028/NIST.IR.8105

Christopher. G. Harris, "Cross-Chain Technologies: Challenges and Opportunties for Blockchain Interoperability," *2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS)*, Berlin, Germany, 2023, pp. 1-6, doi: 10.1109/COINS57856.2023.10189298.

Chuck Easttom, "NTRU and LASH for a Quantum Resistant Blockchain," in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, 2022, 0654–58, https://doi.org/10.1109/CCWC54503.2022.9720790;

Chunying Peng, Haixia Xu, and Peili Li, "Redactable Blockchain Using Lattice-Based Chameleon Hash Function," in *2022 International Conference on Blockchain Technology and Information Security (ICBCTIS)*, 2022, 94–98, https://doi.org/10.1109/ICBCTIS55569.2022.00032;

Deepika Gautam et al., "Blockchain-Assisted Post-Quantum Privacy-Preserving Public Auditing Scheme to Secure Multimedia Data in Cloud Storage," *Cluster Computing* 27, no. 6 (September 1, 2024): 8159–72, https://doi.org/10.1007/s10586-024-04412-8;

Dharani D, Soorya R, and K. Anitha Kumari, "Quantum Resistant Cryptographic Systems for Blockchain Network," in *2023 3rd International Conference on Intelligent Technologies (CONIT)*, 2023, 1–7, https://doi.org/10.1109/CONIT59222.2023.10205646;

Dharminder Chaudhary et al., "Module Lattice-Based Post Quantum Secure Blockchain Empowered Authentication Framework for Autonomous Truck Platooning," *IEEE Access* 12 (2024): 105219–33, https://doi.org/10.1109/ACCESS.2024.3434691;

Dilip Krishnaswamy, "Quantum Blockchain Networks," in *Proceedings of the Twenty-First International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing*, Mobihoc '20 (New York, NY, USA: Association for Computing Machinery, 2020), 327–32, https://doi.org/10.1145/3397166.3412802;

Ding, J., & Lin, X. (2012). A simple provably secure key exchange scheme based on the learning with errors problem. *IACR Cryptology ePrint Archive, 2012*(688). https://ia.cr/2012/688

Ducas, L., Bos, J. W., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., & Seiler, G. (2018). CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 353–367). IEEE. https://doi.org/10.1109/EuroSP.2018.00032

Ducas, L., Bos, J. W., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., & Seiler, G. (2018). CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 353–367). IEEE. https://doi.org/10.1109/EuroSP.2018.00032

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

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

Fujisaki, E., & Okamoto, T. (2017). Secure digital signatures based on learning with errors and its applications to blockchain. *Journal of Cryptology, 30*(2), 101–122. https://doi.org/10.1007/s00145-016-9235-7

G. M. Faruk Ahmed et al., "Enhancing E-KYC Security and Privacy: Harnessing Quantum Computing and Blockchain in Web 3.0," *Distrib. Ledger Technol.* 3, no. 4 (December 22, 2024): 29:1-29:23, https://doi.org/10.1145/3686166;

Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. In *International Algorithmic Number Theory Symposium (ANTS-III)* (pp. 267–288). Springer.

Hui Chen, "Quantum Relay Blockchain and Its Applications in Key Service," in *Proceedings of the 2020 4th International Conference on Cryptography, Security and Privacy*, ICCSP 2020 (New York, NY, USA: Association for Computing Machinery, 2020), 95–99, https://doi.org/10.1145/3377644.3377657;

Huifang Yu and Xiaoping Bai, "Identity-Based Searchable Attribute Signcryption in Lattice for a Blockchain-Based Medical System," *Frontiers of Information Technology & Electronic Engineering* 25, no. 3 (March 1, 2024): 461–71, https://doi.org/10.1631/FITEE.2300248;

Ishita Sawhney, Saurabh Kumar Singh, and Shilpi Sharma, "Biometric Verification Using Blockchain and Quantum Computing," in *2024 4th International Conference on Technological Advancements in Computational Sciences (ICTACS)*, 2024, 1019–26, https://doi.org/10.1109/ICTACS62700.2024.10840605;

Jisha Mary Jose and Panchami V, "A Survey on Consensus Algorithms in Blockchain Based on Post Quantum Cryptosystems," in *2022 5th International Conference on Computational Intelligence and Networks (CINE)*, 2022, 1–6, https://doi.org/10.1109/CINE56307.2022.10037353;

Kai Schärer and Marco Comuzzi, "The Quantum Threat to Blockchain: Summary and Timeline Analysis," *Quantum Machine Intelligence* 5, no. 1 (April 24, 2023): 19, https://doi.org/10.1007/s42484-023-00105-4;

Kanupriya Jain et al., "Quantum Resistant Blockchain-Based Architecture for Secure Medical Data Sharing," in *2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, 2024, 1400–1407, https://doi.org/10.1109/ICAAIC60222.2024.10575286;

Kaushal Shah, Manav Ukani, and Sahaj Bhadja, "A Detailed Exploration to Quantum Resistant Blockchain Technology," in *2024 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, 2024, 1–6, https://doi.org/10.1109/CONECCT62155.2024.10677253;

Khodaiemehr, H., Bagheri, K., & Feng, C. (2023). Navigating the quantum computing threat landscape for blockchains: A comprehensive survey. *TechRxiv*. https://doi.org/10.36227/techrxiv.24136440.v1

Kiltz, E., Ducas, L., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2018*(1), 238-268. https://doi.org/10.13154/tches.v2018.i1.238-268

Kiltz, E., Ducas, L., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018*(1), 238-268. https://doi.org/10.13154/tches.v2018.i1.238-268

Lucy Sharma and Arun Mishra, "Analysis of Crystals-Dilithium for BlockChain Security," in *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*, 2021, 160–65, https://doi.org/10.1109/ICSCCC51823.2021.9478087;

Mahendra Kumar Shrivas et al., "Quantum-Resistant University Credentials Verification System on Blockchain," in *2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON)*, 2022, 1–6, https://doi.org/10.1109/NIGERCON54645.2022.9803153;

Manas Patil et al., "Doc Vault - A Blockchain and Lattice-Cryptography Based Secure Document Storage Platform," in *2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, 2024, 1–7, https://doi.org/10.1109/ETNCC63262.2024.10767517;

Marcos Allende et al., "Quantum-Resistance in Blockchain Networks," *Scientific Reports* 13, no. 1 (April 6, 2023): 5664, https://doi.org/10.1038/s41598-023-32701-6;

Maxime Buser et al., "A Survey on Exotic Signatures for Post-Quantum Blockchain: Challenges and Research Directions," *ACM Comput. Surv.* 55, no. 12 (March 2, 2023): 251:1-251:32, https://doi.org/10.1145/3572771;

Minghui Xu et al., "Exploring Blockchain Technology through a Modular Lens: A Survey," *ACM Comput. Surv.* 56, no. 9 (May 8, 2024): 242:1-242:39, https://doi.org/10.1145/3657288;

Muhammad Zohaib, Fahad S. Altuwaijri, and Sami Hyrynsalmi, "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 2024 (New York, NY, USA: Association for Computing Machinery, 2024), 27–34, https://doi.org/10.1145/3663531.3664755;

Muhammed F. Esgin et al., "A New Look at Blockchain Leader Election: Simple, Efficient, Sustainable and Post-Quantum," in *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security*, ASIA CCS '23 (New York, NY, USA: Association for Computing Machinery, 2023), 623–37, https://doi.org/10.1145/3579856.3595792;

Muhammed F. Esgin, Ron Steinfeld, and Raymond K. Zhao, "MatRiCT+: More Efficient Post-Quantum Private Blockchain Payments," in *2022 IEEE Symposium on Security and Privacy (SP)*, 2022, 1281–98, https://doi.org/10.1109/SP46214.2022.9833655;

Nday Kabulo Sinai and Hoh Peter In, "Performance Evaluation of a Quantum-Resistant Blockchain: A Comparative Study with Secp256k1 and Schnorr," *Quantum Information Processing* 23, no. 3 (March 6, 2024): 99, https://doi.org/10.1007/s11128-024-04272-6;

Peikert, C. (2016). A decade of lattice cryptography. *Foundations and Trends® in Theoretical Computer Science, 10*(4), 283–424. https://doi.org/10.1561/0400000074

Peng Duan and Bo Zhou, "Post Quantum Identity Authentication Mechanism in Blockchain," in *Proceedings of the 8th International Conference on Communication and Information Processing*, ICCIP '22 (New York, NY, USA: Association for Computing Machinery, 2023), 136–41, https://doi.org/10.1145/3571662.3571682;

Prithwi Bagchi et al., "Public Blockchain-Envisioned Security Scheme Using Post Quantum Lattice-Based Aggregate Signature for Internet of Drones Applications," *IEEE Transactions on Vehicular Technology* 72, no. 8 (August 2023): 10393–408, https://doi.org/10.1109/TVT.2023.3260579;

Prithwi Bagchi et al., "Quantum Safe Lattice-Based Single Round Online Collaborative Multi-Signature Scheme for Blockchain-Enabled IoT Applications," *ACM Trans. Sen. Netw.*, January 28, 2025, https://doi.org/10.1145/3715696;

Rahat Naz and Dr. Anuj Kumar, "Surveying Quantum-Proof Blockchain Security: The Era of Exotic Signatures," in *Proceedings of the 25th International Conference on Distributed Computing and Networking*, ICDCN '24 (New York, NY, USA: Association for Computing Machinery, 2024), 412–17, https://doi.org/10.1145/3631461.3631949;

Rahul Saha et al., "A Blockchain Framework in Post-Quantum Decentralization," *IEEE Transactions on Services Computing* 16, no. 1 (January 2023): 1–12, https://doi.org/10.1109/TSC.2021.3116896;

Regev, O. (2005). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM), 56*(6), 1–40. https://doi.org/10.1145/1060590.1060603

Regev, O. (2005). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM), 56*(6), 1–40. https://doi.org/10.1145/1060590.1060603

Sarra Cherbal et al., "Security in Internet of Things: A Review on Approaches Based on Blockchain, Machine Learning, Cryptography, and Quantum Computing," *The Journal of Supercomputing* 80, no. 3 (February 1, 2024): 3738–3816, https://doi.org/10.1007/s11227-023-05616-2;

Sha Xie et al., "Blockchain Data Sharing Scheme Based on Quantum Re-Encryption," *Quantum Information Processing* 23, no. 8 (July 25, 2024): 285, https://doi.org/10.1007/s11128-024-04466-y;

Shashank Joshi, Arhan Choudhury, and R. I. Minu, "Quantum Blockchain-Enabled Exchange Protocol Model for Decentralized Systems," *Quantum Information Processing* 22, no. 11 (November 7, 2023): 404, https://doi.org/10.1007/s11128-023-04156-1;

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS)* (pp. 124–134). IEEE. https://doi.org/10.1109/SFCS.1994.365700

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS)* (pp. 124–134). IEEE. https://doi.org/10.1109/SFCS.1994.365700

Shtwai Alsubai et al., "A Blockchain-Based Hybrid Encryption Technique with Anti-Quantum Signature for Securing Electronic Health Records," *Complex & Intelligent Systems* 10, no. 5 (October 1, 2024): 6117–41, https://doi.org/10.1007/s40747-024-01477-1;

Sunil Prajapat et al., "Quantum-Safe Blockchain-Assisted Data Encryption Protocol for Internet of Things Networks," *Cluster Computing* 28, no. 1 (October 14, 2024): 5, https://doi.org/10.1007/s10586-024-04688-w;

Tannu Sharma et al., "Post Quantum Blockchain Based Lightweight Edge Server Handover Authentication Key Agreement Protocol for Vehicular Communication System," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2023, 1–6, https://doi.org/10.1109/ICCCNT56998.2023.10306504;

Wei Cui, Tong. Dou and Shilu. Yan, "Threats and Opportunities: Blockchain meets Quantum Computation," *2020 39th Chinese Control Conference (CCC)*, Shenyang, China, 2020, pp. 5822-5824, doi: 10.23919/CCC50068.2020.9189608.

Yang, Z., Alfauri, H., Farkiani, B., Jain, R., Pietro, R. D., & Erbad, A. (2024). A survey and comparison of post-quantum and quantum blockchains. *IEEE Communications Surveys & Tutorials, 26*(2), 967–1002. https://doi.org/10.1109/COMST.2023.3325761

Yang, Z., Alfauri, H., Farkiani, B., Jain, R., Pietro, R. D., & Erbad, A. (2024). A survey and comparison of post-quantum and quantum blockchains. *IEEE Communications Surveys & Tutorials, 26*(2), 967–1002. https://doi.org/10.1109/COMST.2023.3325761

Yingpan Kuang et al., "Blockchain Based Lightweight Authentication Scheme for Internet of Things Using Lattice Encryption Algorithm," *Computer Standards & Interfaces* 93 (April 1, 2025): 103981, https://doi.org/10.1016/j.csi.2025.103981;

Yuhan Luo et al., "When Secure Data Sharing Meets Blockchain: Overview, Challenges and Future Prospects," in *Proceedings of the 2022 4th International Conference on Blockchain Technology*, ICBCT '22 (New York, NY, USA: Association for Computing Machinery, 2022), 1–8, https://doi.org/10.1145/3532640.3532641.

Yulong Gao, Xueting Chen, and Wenqian Shang, "A Lattice-Based Linkable Ring Signature Scheme for Blockchain Privacy Protection," in *2024 IEEE/ACIS 27th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 2024, 76–80, https://doi.org/10.1109/SNPD61259.2024.10673921;

Yunjia Quan, "Improving Bitcoin's Post-Quantum Transaction Efficiency With a Novel Lattice-Based Aggregate Signature Scheme Based on CRYSTALS-Dilithium and a STARK Protocol," *IEEE Access* 10 (2022): 132472–82, https://doi.org/10.1109/ACCESS.2022.3227394;

Zhen Zhang, Huiyan Chen, and Yufan Chen, "A Provable Secure Signature in the Quantum Random Oracle Model," in *2022 International Conference on Blockchain Technology and Information Security (ICBCTIS)*, 2022, 43–46, https://doi.org/10.1109/ICBCTIS55569.2022.00021;

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352–375. https://doi.org/10.1504/IJWGS.2018.095647

Zihe Huang, "Incentive Mechanism Design for Joint Resource Allocation in Post-Quantum Blockchain-Based Federated Learning," in *2023 International Conference on Electronics and Devices, Computational Science (ICEDCS)*, 2023, 447–51, https://doi.org/10.1109/ICEDCS60513.2023.00086