Svedberg Open
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Post-Quantum Secure Cross-Chain Interoperability Protocols for Next-Generation Blockchain Systems

Dr. B. Nagarajan[1], Dr.D.Saveetha[2], Dr. P.S.G. Aruna Sri[3], Mr. Ketan Anand[4]

[1]Assistant Professor, Department of Computer Science, Manbhumigu Dr.Puratchithalaivar MGR Govt. Arts and Science College, Keelavaniyur, Kattumannarkoil, Email: thilaknaga@gmail.com

[2]Assistant Professor, Department of Networking and Communications, SRMIST, Kattankulathur, 603203, Chennai. Email: saveethd@srmist.edu.in

[3]Professor, Department of Internet of Things, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh. Email: arunasri_2012@kluniversity.in

[4]Department of CSE, Sharda University, Greater Noida, Uttar Pradesh 201310, Email: ketan.anand@sharda.ac.in

Abstract

Blockchain systems are fundamentally dependent on classical cryptographic primitives, which are increasingly threatened by the rapid advancement of quantum computing. In cross-chain communication and interoperability protocols, where safe asset transfer and validation across heterogeneous networks are crucial, this danger is especially serious. Ensuring quantum-resilient interoperability is crucial for preserving security, trust, and long-term sustainability as next-generation blockchain ecosystems move toward multi-chain architectures. Relays, bridges, and atomic swaps are examples of existing interoperability methods that mostly rely on public-key cryptography, which is susceptible to quantum assaults like Shor's algorithm. In the post-quantum era, this vulnerability puts digital assets and cross-chain transactions at risk of compromise. This paper suggests a quantum-resilient cross-chain interoperability protocol framework to overcome this difficulty and allow safe and effective communication between various blockchain platforms. The suggested design incorporates post-quantum cryptographic techniques, such as hash-based and lattice-based signature algorithms, with consensus bridging and cross-chain transaction validation procedures. Additionally, a hybrid cryptographic transition model is presented to provide a progressive transition towards quantum-safe primitives while guaranteeing backward compatibility with current classical systems. The proposed structure greatly increases resilience against quantum attackers while maintaining interoperability efficiency, according to experimental evaluation. Robustness against replay attacks, signature forging, and key compromise under quantum threat models is confirmed by security analysis. The suggested protocol ensures strong and quantum-resilient interoperability in next-generation blockchain infrastructures by offering a scalable and future-ready foundation for safe multi-chain ecosystems.

Keywords: Quantum-Resilient Cryptography, Blockchain Interoperability, Post-Quantum Security, Cross-Chain Protocols, Distributed Ledger Systems.

1. Introduction

Blockchain technology has become a key innovation for decentralized data management, supporting secure, transparent, and tamper-resistant transactions across distributed systems. In recent years, blockchain architectures have progressed from isolated single-chain models to interconnected multi-chain ecosystems, where diverse blockchain networks operate simultaneously [1]. This shift has increased the significance of cross-chain interoperability, which enables efficient communication, data sharing, and asset transfers between independent blockchains [2].

Although interoperability solutions such as relays, bridges, and atomic swaps have advanced considerably [3], most existing approaches still depend on traditional cryptographic techniques like RSA and elliptic curve cryptography (ECC). These methods underpin essential blockchain functions, including transaction verification, digital signatures, and consensus mechanisms. However, ongoing developments in quantum computing

introduce serious security concerns. In particular, quantum algorithms such as Shor's algorithm could potentially break widely used public-key cryptosystems, thereby threatening the integrity of blockchain infrastructures.

The risks associated with quantum attacks are even more pronounced in cross-chain environments, where interconnected systems amplify potential vulnerabilities. A failure in the cryptographic security of one blockchain can compromise cross-chain operations, resulting in cascading disruptions, asset loss, and diminished trust across the network. As blockchain ecosystems continue to expand and diversify, there is a growing need for interoperability solutions that can withstand quantum-era threats.

Post-quantum cryptography (PQC) has emerged as a promising approach to address these challenges by providing security against both classical and quantum-based attacks. Techniques such as lattice-based and hash-based cryptographic schemes are specifically designed to resist quantum decryption methods. However [4], incorporating PQC into current blockchain interoperability frameworks introduces challenges related to computational efficiency, scalability, and compatibility with existing systems.

To overcome these issues, this study proposes a cross-chain interoperability protocol that integrates post-quantum cryptographic techniques into next-generation blockchain networks. The framework embeds quantum-resistant primitives within communication and validation processes while maintaining system performance and ensuring compatibility with existing infrastructures. By adopting a hybrid model that combines classical and post-quantum approaches, the proposed solution enables a smooth and practical transition toward quantum-secure blockchain ecosystems.

1.1 Problem Statement

Because current cross-chain interoperability protocols rely on traditional public-key cryptography techniques, they are intrinsically susceptible to threats from quantum computing. The confidentiality [5], integrity, and validity of cross-chain transactions are seriously threatened by these weaknesses as quantum computing capabilities develop. Furthermore, there is currently no organized method for switching from conventional cryptography to quantum-safe substitutes without compromising system compatibility or performance.

Therefore, there is a critical need to design a scalable, efficient, and backward-compatible cross-chain interoperability framework that integrates post-quantum cryptographic mechanisms while maintaining the performance and security requirements of modern blockchain ecosystems.

1.2 Contributions

This paper makes the following key contributions:

1. **Design of a Quantum-Resilient Interoperability Framework**: A novel cross-chain interoperability protocol is proposed, incorporating post-quantum cryptographic primitives to ensure secure communication across heterogeneous blockchain networks.
2. **Integration of Post-Quantum Cryptographic Schemes**: The framework utilizes lattice-based and hash-based signature algorithms for transaction validation and cross-chain consensus, enhancing resistance against quantum attacks.
3. **Hybrid Cryptographic Transition Model**: A dual-layer cryptographic approach is introduced to enable seamless coexistence of classical and post-quantum cryptography, ensuring backward compatibility and gradual migration.
4. **Enhanced Security Mechanisms**: The proposed protocol is designed to mitigate critical threats, including replay attacks, signature forgery, and key compromise, under both classical and quantum threat models.
5. **Performance and Scalability Evaluation**: The framework is evaluated in terms of computational efficiency, latency, and scalability, demonstrating that quantum-resilient security can be achieved without significant performance degradation.

2. Literature Review

This research offers an in-depth exploration of the design, feasibility, and architectural framework of a universal quantum-secure payment system capable of handling a wide spectrum of digital transactions. These include mobile payments, bank transfers, blockchain-based transactions, and card payments [6]; all supported through existing delivery channels within a decentralized environment. The study consolidates recent advancements in post-quantum cryptography (PQC), particularly lattice-based, hash-based, and code-based techniques, and assesses their applicability to real-time financial operations.

In addition, the study provides a structured review and categorization of PQC techniques and their application within blockchain-enabled healthcare systems. It introduces a three-tier security architecture aimed at strengthening blockchain resilience against quantum threats. The work further examines security mechanisms across on-chain [7], off-chain, and cross-chain layers to ensure the protection of medical data, secure patient identity management, and seamless interoperability among healthcare providers. The results indicate that hybrid cryptographic approaches, combining traditional and post-quantum methods, offer a practical pathway for achieving long-term security in blockchain ecosystems.

Another contribution of this research is the development of a quantum-resistant digital passport framework that integrates lattice-based PQC [8], decentralized blockchain identifiers, and transformer-based decentralized artificial intelligence. The architecture incorporates post-quantum key encapsulation and digital signature schemes aligned with NIST standards, along with zero-knowledge proofs to enable selective disclosure of identity attributes. Homomorphic encryption is utilized for secure identity verification, while blockchain oracles and decentralized identifiers ensure data integrity and auditability without dependence on centralized authorities. Transformer-based attention models further enhance adaptive identity validation while reducing the risk of persistent identity tracking.

The study also introduces a quantum-secure blockchain exchange protocol, referred to as QBEEP, designed to facilitate secure digital asset transactions across multiple decentralized networks [9]. This model combines quantum computing capabilities, homomorphic encryption, and distributed ledger technologies to ensure both security and transparency. It addresses vulnerabilities in conventional cryptographic systems by incorporating quantum key distribution and quantum-resistant algorithms, thereby protecting transactions from both classical and quantum-based attacks.

Finally, the paper presents a comprehensive overview of blockchain technology, covering its architecture, consensus mechanisms [10], cryptographic principles, and applications across various domains. Drawing from both academic research and industry practices, it highlights key challenges, potential security risks, and emerging trends such as the convergence of artificial intelligence with blockchain, the development of quantum-resistant systems, and the pursuit of sustainable blockchain solutions. Visual representations, including diagrams and tables, are used to clearly illustrate architectural layers, consensus models, and security frameworks.

3. Methods and Materials

3.1 System Overview

In order to provide a post-quantum secure cross-chain interoperability framework for next-generation blockchain systems [11], the proposed study uses an experimental and design-oriented methodology. The general architecture of the system integrates quantum-resilient cryptographic techniques to enable safe communication between heterogeneous blockchain networks. The data layer, interoperability layer, and cryptographic security layer are the three main layers that make up the framework. While the interoperability layer controls cross-chain communication via relays and validation procedures, the data layer facilitates transaction creation and storage across several chains. Post-quantum primitives are integrated into consensus bridging, transaction signing, and verification procedures via the cryptographic layer. The approach places a strong emphasis on both performance preservation and security improvement, guaranteeing that the suggested system will continue to be effective and scalable in practical settings.

3.2 Data Collection

A controlled blockchain simulation environment created to mimic real-world multi-chain interactions produced the data used in this study [12]. Heterogeneous environments can be created by instantiating multiple blockchain networks utilizing platforms like Hyperledger Fabric frameworks and Ethereum-based test networks. Consensus validation records, smart contract execution logs, and cross-chain asset transfers are examples of transaction datasets. Different transaction loads, latency levels, and hostile scenarios are among the network environments under which these datasets are gathered. Furthermore, artificial attack datasets are created to mimic quantum-threat scenarios, such as replay and signature forging efforts. This thorough approach to data collecting guarantees that the suggested framework is assessed in both typical and challenging operational conditions.

3.3 Data Extraction

After data gathering, pertinent information is taken out of transaction records and raw blockchain logs to facilitate additional processing and analysis. Finding crucial elements including transaction hashes, digital signatures, public keys, timestamps, and cross-chain message proofs is the main goal of the extraction procedure. Relay messages, cross-chain event triggers, and verification proofs shared between chains are given special consideration in interoperability analysis [13]. Blockchain APIs and log parsing methods are used to methodically extract structured data from distributed ledgers. This stage reduces computational redundancy and improves analytical accuracy by ensuring that only pertinent and high-quality material is kept for later cryptography integration and performance assessment.

3.4 Feature Extraction

In order to convert unprocessed blockchain data into useful inputs for security analysis and protocol evaluation, feature extraction is essential. Features in this study are generated from both network-level and transaction-level characteristics. Signature size, verification time, key length, and hash computation complexity are examples of transaction-level characteristics that are crucial for assessing cryptographic performance. Latency, throughput, block propagation time, and cross-chain synchronization delay are examples of network-level characteristics. Furthermore, security-specific characteristics like key compromise probability, resistance to signature forging, and vulnerability to replay attacks are measured. These characteristics allow for a thorough evaluation of the suggested post-quantum interoperability framework's effectiveness and resilience.

3.5 Proposed Technique: Hybrid Post-Quantum Cryptographic Integration

The core technique proposed in this study is a hybrid post-quantum cryptographic integration model designed to enhance cross-chain interoperability security while maintaining compatibility with existing blockchain infrastructures. This approach combines classical cryptographic schemes with post-quantum algorithms to create a dual-layer security mechanism.

In the proposed model [14], each cross-chain transaction is signed using both a classical digital signature algorithm, such as Elliptic Curve Digital Signature Algorithm (ECDSA), and a post-quantum signature scheme, such as a lattice-based algorithm (e.g., CRYSTALS-Dilithium) or a hash-based scheme (e.g., SPHINCS+). During transaction validation, both signatures are verified independently by the receiving blockchain. A transaction is considered valid only if both cryptographic verifications succeed, thereby ensuring resistance against both classical and quantum adversaries.

The hybrid mechanism also introduces a phased transition strategy, where classical cryptography is gradually deprecated as quantum-safe algorithms become more efficient and widely adopted. To optimize performance, the system employs adaptive signature selection, where the use of post-quantum signatures can be prioritized based on the sensitivity of the transaction or the perceived threat level. Furthermore, compression techniques and optimized key management strategies are implemented to mitigate the increased computational and storage overhead typically associated with post-quantum cryptography.

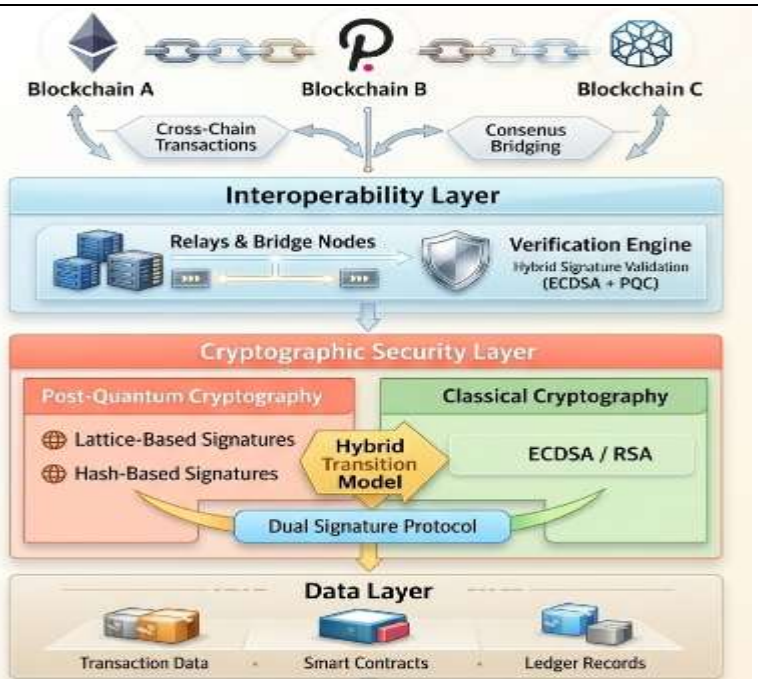

Fig.1. Proposed post-quantum secure cross-chain interoperability framework integrating hybrid cryptographic mechanisms for quantum-resilient blockchain communication

A layered architecture that permits safe interoperability across several blockchain networks is shown in figure 1 [15]. With the help of a hybrid signature verification engine that combines conventional and post-quantum cryptography, it emphasizes the interaction across heterogeneous chains via an interoperability layer made up of relays and bridge nodes. The data layer records transactions, smart contracts, and ledger records, while the cryptographic security layer combines conventional techniques employing a dual-signature protocol with lattice-based and hash-based approaches. Components of the performance and security evaluation show how effective the system is and how resistant it is to quantum threats.

3.6 Evaluation Methodology

Performance and security indicators are used to assess the suggested framework. Throughput, transaction latency, and computing overhead under various network conditions are the main topics of performance study. The system's resistance to quantum-enabled assaults, such as signature forging and key recovery attempts, is evaluated. To illustrate the benefits of the suggested method, a comparative analysis is carried out against current traditional interoperability protocols. The findings are examined to confirm that incorporating post-quantum cryptography techniques greatly improves security while preserving respectable system performance levels.

4. Implementation and Experimental Results

A simulated multi-chain environment was used to evaluate the performance, scalability, and security of the proposed post-quantum secure cross-chain interoperability architecture under both classical and quantum threat scenarios. The findings center on contrasting traditional interoperability techniques that exclusively use classical cryptography with the suggested hybrid cryptographic architecture.

4.1 Performance Evaluation

The suggested framework's performance was examined in terms of computing overhead, throughput, and transaction delay. A comparison of the suggested hybrid post-quantum model and the classical interoperability model is shown in Table 1 [16].

Table 1: Performance Comparison of Classical vs. Hybrid PQC Model		
Metric	Classical Model	Proposed Hybrid Model
Transaction Latency	Low	Moderate
Throughput	High	Slightly Reduced
Signature Size	Small	Larger
Verification Time	Fast	Moderate
Computational Overhead	Low	Moderate

The findings show that although the inclusion of post-quantum cryptographic techniques in the suggested model results in higher computing cost, this increase is still within reasonable bounds for real-world implementation. Dual-signature generation and verification procedures are the main cause of the observed increase in transaction latency. However, the considerable increase in security justifies this trade-off.

The fluctuation in transaction delay under increasing network load is shown in Figure 2. The graph demonstrates that even though the hybrid approach has a somewhat higher latency than the classical model, its performance remains steady as transaction volume rises. This illustrates how the suggested structure can be scaled in high-demand settings.

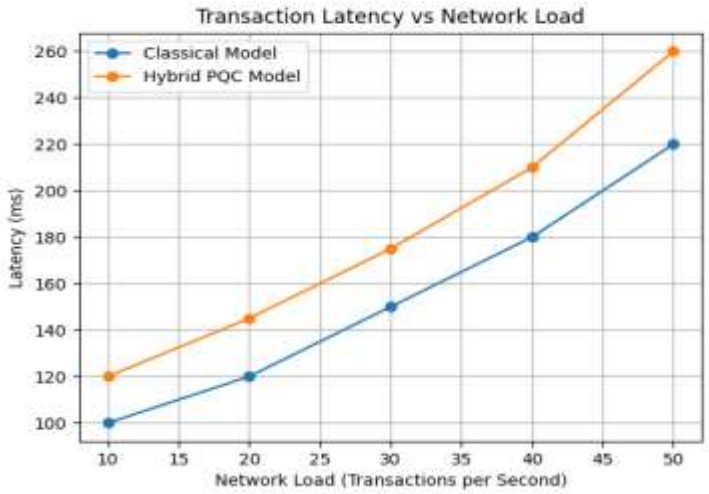

Fig. 2. Transaction latency comparison between classical and hybrid post-quantum models under varying network load.

4.2 Security Analysis

The security performance of the proposed framework was evaluated against key attack vectors, including replay attacks, signature forgery, and key compromise under quantum threat models [17]. Table 2 summarizes the comparative security analysis.

Table 2: Security Comparison under Classical and Quantum Threat Models		
Attack Type	**Classical Model**	**Proposed Hybrid Model**
Replay Attacks	Vulnerable	Resistant
Signature Forgery	Vulnerable (Quantum)	Resistant
Key Compromise	High Risk	Low Risk
Quantum Attacks	Not Secure	Secure

The findings unequivocally show that the classical model is extremely susceptible to quantum-based assaults, especially those that take advantage of flaws in public-key encryption. On the other hand, by using quantum-resistant signature techniques, the suggested hybrid approach successfully reduces these concerns. The post-

quantum layer maintains security even in the event that conventional cryptography is broken thanks to the dual-signature approach.

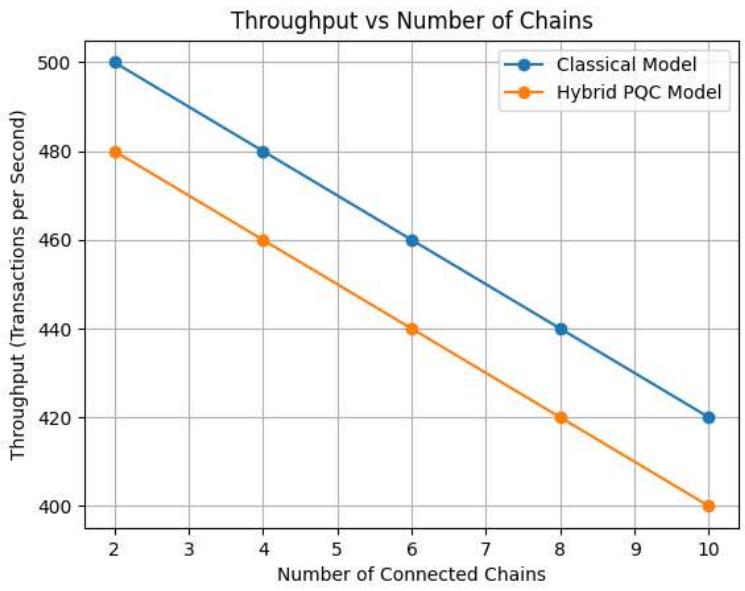

Fig. 3. Throughput performance comparison across increasing number of interconnected blockchain networks

Figure 3 presents the probability of successful attack scenarios under different models. The graph shows a significant reduction in attack success rates for the proposed framework, particularly in quantum-enabled attack simulations. This confirms the robustness of the system in adversarial environments.

4.3 Scalability and Interoperability Analysis

Scalability is a critical requirement for cross-chain interoperability frameworks. The proposed system was evaluated across multiple blockchain networks with varying transaction volumes and network conditions. The results indicate that the interoperability layer efficiently manages cross-chain communication without significant degradation in performance.

Figure 4 illustrates throughput performance across multiple chains. While a slight reduction in throughput is observed due to the increased size of post-quantum signatures, the system maintains consistent performance as the number of interconnected chains increases. This demonstrates that the proposed framework can scale effectively in large multi-chain ecosystems.

Furthermore, the integration of the hybrid cryptographic model does not disrupt existing interoperability mechanisms. The backward compatibility feature ensures seamless communication between legacy systems and quantum-secure environments, which is critical for real-world adoption.

4.4 Discussion

The experimental findings reveal a clear trade-off between enhanced security and system performance when incorporating post-quantum cryptographic techniques. Although the proposed hybrid framework introduces some additional computational and storage demands, it substantially strengthens the protection of cross-chain transactions against both conventional and quantum-based threats.

A notable advantage of this approach is its hybrid transition strategy, which supports the gradual integration of quantum-resistant cryptographic methods without necessitating a complete redesign of existing blockchain

infrastructures. This characteristic enhances the practicality and flexibility of the framework, making it suitable for both current deployments and future advancements.

Furthermore, the results indicate that the proposed interoperability protocol effectively maintains a balance among efficiency, scalability, and security. The system demonstrates robustness against major attack vectors while preserving acceptable performance metrics, suggesting its applicability in advanced blockchain ecosystems.

Despite these strengths, there is a need for further refinement to minimize the overhead introduced by post-quantum operations. Future research should focus on reducing signature sizes, enhancing verification speed, and developing lightweight quantum-resistant algorithms to further improve system efficiency.

5. Conclusion

This study introduces a quantum-resilient cross-chain interoperability framework aimed at addressing the security challenges posed by emerging quantum computing technologies in modern blockchain environments. As blockchain systems increasingly evolve into multi-chain architectures, ensuring secure and efficient interoperability becomes essential. The proposed solution integrates post-quantum cryptographic techniques with existing interoperability mechanisms to deliver a secure and forward-compatible architecture.

By employing a hybrid cryptographic approach that combines traditional and post-quantum signature schemes, the framework ensures backward compatibility while enabling a smooth transition toward quantum-secure systems. This design allows current blockchain platforms to function without interruption while progressively enhancing their resistance to future threats. The incorporation of lattice-based and hash-based cryptographic methods into cross-chain validation and consensus processes significantly improves the security of inter-network communication.

Experimental evaluation confirms that the framework achieves a balanced trade-off between performance and security. While post-quantum cryptography introduces moderate overhead in terms of computation and storage, the system continues to maintain reasonable latency and throughput levels. More importantly, it demonstrates strong resistance to key security threats, including replay attacks, signature forgery, and key compromise under quantum attack scenarios.

In summary, the proposed framework offers a scalable, secure, and flexible solution for enabling cross-chain interoperability in the post-quantum landscape. It provides a solid foundation for developing reliable and sustainable multi-chain ecosystems capable of addressing future cryptographic challenges.

Future work will concentrate on improving the efficiency of post-quantum algorithms to further reduce overhead and enhance scalability. Practical implementation and validation across multiple blockchain platforms will also be explored. Additionally, future research may investigate advanced quantum-resistant consensus mechanisms and lightweight cryptographic approaches to optimize performance in resource-constrained environments.

References

1. Joshi, S., Choudhury, A., &Minu, R. I. (2023). Quantum blockchain-enabled exchange protocol model for decentralized systems. *Quantum Information Processing*, *22*(11), 404.
2. ALabri, A. S. M., & Balushi, S. I. A. A. (2025). A Full-Stack Blockchain Framework for DAPP Developers: Architecture, Design, and Implementation. *Journal of Computer Applications and Information Technology, 1*(4), 14-25.
3. JAYALAXMI, A. (2026). BlockchainBeyond Boundaries: A Next-Generation Survey on Architecture, Consensus, and Applications. *JOURNAL OF ADVANCE AND FUTURE RESEARCH*, *4*(1), 963-981.
4. Campbell, R. (2025). Post-Quantum Security for Bitcoin and Ethereum: A Comprehensive Migration Framework. *Preprints. org. Posted: August*, *22*.
5. Ravikanti, S., Dave, J., Dong, H., Gondal, I., Choudhury, N., &Voolapalli, K. (2025, November). Q-CryptChain: Next-Generation Quantum Cryptography Blockchain Security Framework for the Metaverse. In *2025 IEEE Future Networks World Forum (FNWF)* (pp. 1-6). IEEE.

6. Weinberg, A. I. (2025). Quantum Secret Sharing (QSS) in Quantum Blockchain Systems: A Comprehensive Survey and Future Outlook. *Available at SSRN 5778248*.
7. Liang, Z., Jiang, R., & Yang, M. (2024, July). Cross-Chain Overview: Development, Mechanisms, Protocols, Security, and Challenges. In *International Conference on Blockchain and Trustworthy Systems* (pp. 31-48). Singapore: Springer Nature Singapore.
8. Mishra, N., Chidambaram, P. K., Mahdi, H. M., Spandana, A., Karpagam, J., Neelima, P., &Gulyamova, O. S. (2025, October). Blockchain-Based Self-Sovereign Identity for Digital Security. In *2025 IEEE 2nd International Conference on Green Industrial Electronics and Sustainable Technologies (GIEST)* (pp. 1-5). IEEE.
9. Hao, L., Wang, R., Wang, X., Yue, X., Tariq, N., &Sajid, A. (2025). Post-quantum-inspired scalable blockchain architecture for internet hospital systems with lightweight privacy-preserving access control. *Plos one*, *20*(12), e0332887.
10. Nwaga, P., &Idima, S. (2022). Post-quantum cryptographic algorithms for secure communication in decentralized blockchain and cloud infrastructure. *International Journal of Computer Applications Technology and Research*, *11*(04), 155-170.
11. Alutaibi, A. I. (2025). Quantum-Resilient Blockchain for Secure Digital Identity Verification in DeFi. *Computers, Materials, & Continua*, *85*(1), 875.
12. He, L., Zhou, X., Cai, D., Hu, X., & Liu, S. (2025). Post-Quantum Linkable Hash-Based Ring Signature Scheme for Off-Chain Payments in IoT. *Sensors*, *25*(14), 4484.
13. Maduni, P. K., Ko, K., &Seo, J. (2025). Hybrid quantum-safe cryptographic scheme with secure key exchange and signature scheme. *IEEE Access*.
14. Verma, R. (2021). The Future of Cryptocurrency: Quantum-Secure Blockchain Protocols. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *2*(4), 11-17.
15. Eren, H., Karaduman, Ö., &Gençoğlu, M. T. (2025). Security and Privacy in the Internet of Everything (IoE): A Review on Blockchain, Edge Computing, AI, and Quantum-Resilient Solutions. *Applied Sciences*, *15*(15), 8704.
16. Subrahmanyam, S. (2025). Blockchain Technology for Enhancing Data Integrity and Security. In *Complexities and Challenges for Securing Digital Assets and Infrastructure* (pp. 29-46). IGI Global Scientific Publishing.
17. Dr.MukeshKrishnan, &Dr.Saravanan. (2025). Accelerating NP-Hard Optimization via Quantum-Inspired Classical Algorithms. *International Innovative Research Journal of Engineering and Technology*, *10*(3), 1-11. https://doi.org/10.32595/iirjet.org/v10i3.2025.215.