Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-5 | May-2025 | Page 669-677

Post-Quantum and Interoperable Blockchain Framework for IoT Security

Avanti Sahu
Assistant Professor
Dr. C.V. Raman University, Kota, Bilaspur, Chhattisgarh, India

Abstract
The Internet of Things (IoT) is growing rapidly, connecting billions of devices across homes, industries, cities, and healthcare systems. With this growth comes a major challenge—ensuring secure communication between devices. Traditional encryption methods such as RSA and ECC, though widely used, may not survive future quantum attacks. At the same time, most blockchain-based IoT security models are designed to work within a single platform and lack support for interoperability. This review paper explores how post-quantum cryptography (PQC) and cross-chain blockchain communication can together form a strong, future-ready security framework for IoT systems. We analyze the strengths and weaknesses of PQC algorithms like Kyber, Dilithium, and SPHINCS+, and assess their practicality for low-power IoT devices. The paper also examines blockchain technologies such as Hyperledger Fabric, Ethereum, and Cosmos, comparing their support for smart contracts, scalability, energy usage, and cross-chain data exchange. Through this comparative review, we highlight the research gaps and propose a direction where quantum-resilient encryption and interoperable blockchain networks are integrated to build secure, scalable IoT ecosystems. This work serves as a foundation for researchers and developers aiming to secure next-generation IoT systems against future threats while maintaining flexibility across blockchain platforms.

Keywords: Post-Quantum Cryptography, Blockchain Interoperability, IoT Security, Cross-Chain Communication, Quantum-Resilient Architecture

1. Introduction

The Internet of Things (IoT) has become a key part of modern technology, connecting smart devices in homes, cities, industries, and healthcare. From sensors in farming fields to wearable health monitors, IoT systems are being widely adopted due to their ability to collect, process, and transmit real-time data. However, this rapid growth also brings major security concerns. As more devices connect to networks, the risk of data theft, system tampering, and unauthorized access increases significantly. Blockchain technology has been considered a strong solution for securing IoT environments. It offers a decentralized and tamper-resistant way to manage device identity, ensure data integrity, and enable trust without relying on a central authority. However, most current blockchain systems depend on classical cryptographic methods like RSA and Elliptic Curve Cryptography (ECC), which are believed to be vulnerable in the era of quantum computing. Quantum computers, when matured, could easily break these

encryption methods, leaving IoT systems exposed. Another limitation in the current blockchain-IoT ecosystem is the lack of interoperability. Many blockchain networks operate in isolation, making it difficult for devices across platforms to exchange data securely. In this we explore how **post-quantum cryptography (PQC)** and **interoperable blockchain frameworks** can work together to solve these challenges. It discusses the potential of combining quantum-safe encryption with cross-chain communication protocols to build secure, scalable, and future-proof IoT networks.

2. Need for Post-Quantum Cryptography in IoT

IoT devices are often small, low-powered, and resource-constrained, but they handle sensitive data such as personal health records, location details, and financial information. To protect this data, cryptographic techniques like RSA and Elliptic Curve Cryptography (ECC) are commonly used. However, the development of quantum computing brings a serious threat to these traditional encryption methods.

Quantum computers are expected to solve mathematical problems much faster than classical computers. Algorithms such as Shor's algorithm can break RSA and ECC in seconds once powerful quantum machines become available. This means that all data currently protected by these systems—including IoT device communication—could become readable and vulnerable. Given the long lifecycle of IoT devices, many of which stay active for 10–15 years, it is important to prepare now for a post-quantum world.

Post-quantum cryptography (PQC) is a new field that focuses on developing cryptographic algorithms that can resist attacks from quantum computers. These include lattice-based, hash-based, code-based, and multivariate polynomial-based encryption methods. Among these, lattice-based algorithms like Kyber and Dilithium are considered efficient and suitable for constrained environments like IoT.

Integrating PQC into IoT systems is not just a future consideration—it is an urgent requirement. It ensures long-term data protection, device trust, and system integrity in a future where quantum threats will become real and widespread.

3. Overview of Blockchain for IoT Security

As IoT devices continue to expand in number and variety, securing the data they generate and exchange has become a top priority. Traditional centralized security systems rely on cloud servers and third-party providers to authenticate devices and manage access. However, these centralized models often create single points of failure and become attractive targets for cyberattacks such as DDoS, spoofing, and unauthorized data access.

Blockchain technology offers a decentralized alternative that is highly suitable for securing IoT environments. A blockchain is a distributed ledger system where all transactions are recorded in a tamper-resistant, transparent, and verifiable way. In an IoT context, blockchain can help by offering secure device registration, automated access control using smart contracts, and reliable data auditing.

Several blockchain platforms have been explored for IoT security. Ethereum provides smart contract functionality but faces issues like high energy consumption and transaction delays.

Hyperledger Fabric, on the other hand, supports permissioned networks and is more suitable for enterprise-level IoT systems with known participants. IoTChain and EdgeChain are other examples that aim to combine blockchain with edge computing for faster and localized processing.

Despite these advancements, using blockchain in IoT is not without challenges. Standard blockchain consensus methods like Proof of Work (PoW) require significant computational resources, which are not suitable for low-power IoT devices. Therefore, lightweight consensus protocols such as Practical Byzantine Fault Tolerance (PBFT) and IoT-PBFT have been proposed to reduce latency and energy use while maintaining security.

4. Interoperability in Blockchain Systems

While blockchain has shown great potential in securing IoT networks, most existing solutions are built on isolated or "siloed" platforms. For example, an IoT application using Hyperledger may not be able to communicate directly with another system based on Ethereum or Cosmos. This lack of interoperability is a major challenge, especially when multiple devices and platforms need to share data securely and in real time.

In the real world, IoT systems are highly diverse. A smart city, for instance, may involve sensors for traffic control, waste management, healthcare monitoring, and public safety—all built by different vendors and running on different blockchain infrastructures. Without a way to connect these systems, data exchange becomes limited, and overall system efficiency suffers.

Interoperability in blockchain means that different blockchain networks can interact, exchange data, and perform transactions across platforms without needing a central authority. Technologies like Cosmos (using Inter-Blockchain Communication – IBC) and Polkadot (with relay chains and parachains) have been developed to enable such communication between blockchains.

For IoT, enabling interoperability can improve coordination between devices, reduce system fragmentation, and support more scalable solutions. It also allows organizations to adopt the most suitable blockchain for their needs without being locked into a single provider. However, achieving seamless interoperability is technically complex. Challenges include managing consensus across chains, handling transaction formats, and ensuring security during cross-chain communication.

In future IoT networks, combining interoperable blockchains with post-quantum security will be essential to building systems that are not only safe but also flexible, adaptive, and future-ready.

5. Comparative Review: PQC + Interoperable Blockchain Models

Several research studies and frameworks have addressed either post-quantum cryptography (PQC) or blockchain-based IoT security. However, very few have tried to combine both PQC and blockchain interoperability in one integrated model. This section compares the current state of technologies and highlights how combining these two components can provide a more robust and future-ready solution for IoT security.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-5 | May-2025 | Page 669-677

Post-Quantum Cryptography (PQC) algorithms like Kyber, Dilithium, and SPHINCS+ have been recommended by NIST as quantum-safe alternatives to classical cryptography. Among them, Kyber and Dilithium offer a good balance between security and performance, making them more practical for IoT devices that have limited power and memory.

On the blockchain side, platforms such as Ethereum, Hyperledger Fabric, and Cosmos offer different strengths. Ethereum supports smart contracts but is resource-heavy. Hyperledger Fabric provides permissioned access and is more energy-efficient. Cosmos stands out for its interoperability features, allowing different blockchain networks to exchange data using Inter-Blockchain Communication (IBC).

When we compare existing frameworks like AI-ZKP-IoT or IoTChain, they either focus on privacy using AI or improving on-chain performance. But they lack two critical features: quantum resistance and cross-chain support. A framework that integrates PQC for encryption and interoperability protocols for communication can address both upcoming quantum threats and real-world IoT requirements where multiple blockchains need to work together.

The comparative analysis shows a clear research gap—no current solution fully combines PQC and interoperability in a blockchain-based IoT model. This highlights the importance of future research that brings these two aspects together.

Table 1: Comparative Review of PQC and Interoperable Blockchain Models

Framework / Technology	Post-Quantum Ready	Interoperability	IoT Suitability	Smart Contract Support	Resource Efficiency
AI-ZKP-IoT	No	No	High	Yes	Moderate
IoTChain	No	No	Moderate	Yes	Moderate
Ethereum	No	Limited	Low	Yes	Low
Hyperledger Fabric	No	No	High	Yes	High
Cosmos	No	Yes	Moderate	Yes	Moderate
Proposed Model	Yes	Yes	High	Yes	High

6. Literature Review

With the rise of quantum computing and cross-platform communication demands in Internet of Things (IoT) systems, researchers have increasingly focused on strengthening cryptographic and architectural frameworks. A wide range of recent studies (2024–2025) provide valuable insights into two major directions: post-quantum cryptography (PQC) and interoperable blockchain systems. However, integration of both technologies into a unified IoT security framework remains underexplored.

In the domain of post-quantum cryptography, Rathi et al. [1] presented a lightweight PQC scheme for IoMT systems using Kyber, showing strong quantum resistance and suitability for health data protection. Similarly, Kumar and Sengupta [2] compared multiple PQC algorithms and concluded that Dilithium offers a better balance between performance and energy cost in constrained environments. Hossain et al. [11] and Lee and Han [16] further explored SPHINCS+ and other hash-based schemes for edge devices, confirming their security but

noting computational challenges. Bhatt and Chawla [8] emphasized optimization techniques to make PQC more adaptable to low-powered edge environments.

In blockchain research, Roy et al. [3] proposed an IoT architecture using Cosmos SDK and IBC protocol, enabling cross-chain data exchange between devices. Jain and Prasad [4] showed how Polkadot's relay chain supports secure, interoperable health data sharing. Verma and Rao [20] also analyzed transaction consistency and latency in cross-chain systems, identifying key risks during inter-chain bridge operations. Nath and Verma [9] explored layer-2 solutions for faster cross-chain consensus in sensor networks. Mishra and Sharma [22] built a hybrid blockchain-based access control model for industrial IoT by using role-based tokens.

Several attempts have been made to combine PQC with blockchain security. Deshmukh and Srivastava [5] integrated Kyber encryption into firmware authentication, while Kapoor and Patel [18] created a PQC-enabled smart contract mechanism for verifying grid updates. However, neither solution addresses blockchain interoperability. Zhang and Li [7] laid out foundational work for post-quantum blockchains, but implementation in real-world IoT scenarios was not included. Mehta and Rana [10], as well as Singh and Goel [13], proposed hybrid PQC-blockchain models for smart metering and agriculture, but lacked cross-chain operability.

On the interoperability front, Hussain et al. [19] and Sharma and Thomas [12] advanced multi-chain ledgering for edge devices and identity management, respectively, using Cosmos and Fabric. Arora and Devraj [24] demonstrated secure telemetry in transportation using Dilithium and Tendermint, marking a scalable approach, although their model focused on performance rather than cross-chain logic. Thomas and Sahu [21] introduced lattice-PKE in permissioned blockchains to secure medical records, but again within a single-chain context.

Additional review work by Malhotra and Gupta [15] and Anand et al. [23] highlighted the lack of standardized PQC APIs, and the limited number of field-tested, interoperable, and quantum-resilient blockchain models. Their findings echoed those of Reddy and Banerjee [14], who discussed convergence of PQC and Zero Knowledge Proofs for user authentication in IoT systems. Arguably the most comprehensive survey to date was done by Mehta and Ghosh [25], who confirmed that no current framework fully merges PQC and blockchain interoperability in a deployable IoT solution.

Together, these studies underline a strong research trend toward quantum resistance and platform interoperability in blockchain-based IoT security. Yet, they also clearly show that a fully integrated, scalable, and post-quantum secure cross-chain framework remains a missing piece in the literature. This review paper addresses that gap by synthesizing existing knowledge and guiding future exploration.

7. Challenges and Research Gaps

Despite considerable progress in both post-quantum cryptography (PQC) and blockchain-based IoT security, the integration of these two domains still faces several unresolved challenges. A major gap observed in the literature is the absence of a unified framework that combines post-quantum secure algorithms with interoperable blockchain systems tailored for IoT. While many studies such as those by Mehta and Ghosh [25] and Hossain et al. [11] explore

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-5 | May-2025 | Page 669-677

each domain separately, none fully address their integration in a practical and scalable manner. This creates a critical void, especially considering that IoT systems are expected to operate securely across different blockchain environments in the near future.

Another significant challenge is the resource limitation of IoT devices. Algorithms like Dilithium and SPHINCS+ offer strong quantum resistance but come with large key sizes and high processing demands. As noted by Lee and Han [16], such algorithms are difficult to deploy on edge devices with limited memory and energy resources. Additionally, cross-chain communication—a key element of blockchain interoperability—introduces its own risks. Studies by Verma and Rao [20] highlight that data inconsistency and transaction replay attacks may occur when blockchains like Ethereum, Hyperledger, and Cosmos exchange information via bridges or relays.

Furthermore, real-world implementation and testing of these advanced security models remain limited. While Kapoor and Patel [18] and Deshmukh and Srivastava [5] have demonstrated proof-of-concept integrations, long-term field deployments are still lacking. Energy consumption also remains a concern. As shown by Li et al. [17], combining PQC and blockchain functionalities often increases power requirements, making such systems less suitable for low-power IoT environments. Scalability is another issue—particularly in multi-chain ecosystems where ensuring consistent cryptographic security across varying consensus mechanisms remains a difficult problem, as emphasized by Arora and Devraj [24].

Lastly, there is a lack of standardized APIs and development protocols that would allow seamless integration of PQC algorithms and cross-chain modules into real-world IoT applications. As noted by Malhotra and Gupta [15], this standardization is essential to ensure interoperability not just between blockchains, but also between IoT manufacturers and network providers. Addressing these gaps is critical to developing practical, future-ready IoT ecosystems that are both quantum-secure and blockchain-interoperable.

Table 2: Challenges and Research Gaps in PQC + Interoperable Blockchain for IoT

Challenge / Gap	**Literature Reference**
Lack of integrated PQC + Interoperable Blockchain frameworks	Mehta & Ghosh [25], Hossain et al. [11]
High resource demands of PQC algorithms in IoT devices	Lee & Han [16], Hossain et al. [11]
Security risks in cross-chain communication	Verma & Rao [20], Hussain et al. [19]
Limited real-world deployment and field testing	Deshmukh & Srivastava [5], Kapoor & Patel [18]
Increased energy consumption in hybrid systems	Li et al. [17]
Scalability issues in multi-chain IoT environments	Roy et al. [3], Arora & Devraj [24]
Lack of standardized APIs and protocols	Malhotra & Gupta [15]

8. Future Directions

As IoT ecosystems become more complex and security-critical, especially in applications such as smart healthcare, autonomous transportation, and industrial automation, the need for

quantum-resilient and interoperable blockchain frameworks will only grow. Future research must therefore focus on building integrated architectures that combine post-quantum cryptographic (PQC) primitives with cross-chain blockchain interoperability to secure IoT environments at scale.

One promising direction is the development of lightweight PQC algorithms specifically optimized for constrained IoT devices. Existing algorithms such as Kyber, Dilithium, and SPHINCS+ should be further tuned to reduce key sizes, computational cost, and energy consumption without compromising quantum resistance. Future work should explore hybrid cryptographic stacks, combining both classical and post-quantum components, which can offer a transition-friendly path for real-world IoT deployments.

Another important area is the standardization of interoperable blockchain protocols that are compatible with PQC-based signatures and encryption schemes. This includes extending frameworks like Cosmos, Polkadot, and Hyperledger to support post-quantum secure bridges, consensus protocols, and identity mechanisms. Moreover, researchers should work on unified API layers and SDKs that simplify the integration of PQC and blockchain modules into existing IoT platforms.

Future studies must also focus on real-world pilot deployments and cross-domain testbeds to evaluate performance, scalability, and attack resistance. For instance, simulating smart grid communication or cross-border logistics using a PQC-interoperable blockchain framework can help validate practical feasibility. Integration with AI-based anomaly detection and zero-knowledge proofs (ZKPs) could further enhance privacy and data integrity in decentralized IoT ecosystems.

Ultimately, a collaborative effort among cryptographers, blockchain architects, IoT developers, and policy-makers will be required to bring forward a secure, scalable, and quantum-resilient future for the Internet of Things. By bridging the existing gaps and capitalizing on emerging technologies, future frameworks can ensure long-term trust, resilience, and cross-platform operability in the face of evolving cybersecurity threats.

9. Conclusion

In this review, we examined the emerging landscape of post-quantum cryptography (PQC) and interoperable blockchain frameworks for securing Internet of Things (IoT) ecosystems. With the advancement of quantum computing and the increasing heterogeneity of IoT platforms, traditional security mechanisms are proving inadequate. The reviewed literature from 2024 and early 2025 reveals significant efforts toward developing both quantum-resistant cryptographic schemes and cross-chain blockchain architectures. However, a key observation is that most current research treats these domains in isolation, with very limited integration across both technological fronts.

While various studies have proposed promising PQC solutions suitable for resource-constrained IoT devices, challenges such as high memory consumption, computational complexity, and energy overhead still persist. Similarly, blockchain interoperability frameworks like Cosmos and Polkadot offer strong capabilities for cross-chain communication, but they lack native support for post-quantum security. Furthermore, real-world

implementations of combined PQC and interoperable blockchain models are scarce, and standardization is still in its infancy.

To address these gaps, future research must focus on building holistic, scalable, and energy-efficient frameworks that unify PQC and blockchain interoperability within the IoT context. This includes algorithmic optimization, development of lightweight protocols, standardized APIs, and practical field deployments. A multi-disciplinary approach—combining cryptography, blockchain engineering, IoT design, and cybersecurity policy—will be critical in developing robust solutions capable of withstanding both classical and quantum-era threats.

References

[1] N. Rathi, P. Singh, and S. Thakur, "Lightweight Post-Quantum Cryptography for Secure IoMT," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 1542–1553, Jan. 2024.

[2] A. Kumar and A. Sengupta, "Analyzing PQC Algorithm Suitability for IoT Devices," *ACM Trans. Embedded Comput. Syst.*, vol. 23, no. 1, Feb. 2024.

[3] R. Roy, K. Das, and V. Sharma, "A Decentralized Interoperable IoT Framework Using Cosmos," *Sensors*, vol. 24, no. 3, Mar. 2024.

[4] R. Jain and R. Prasad, "Polkadot-Based Secure Data Exchange for IoT Healthcare Systems," *IEEE Access*, vol. 12, pp. 31298–31310, Apr. 2024.

[5] S. Deshmukh and R. Srivastava, "Firmware Authentication in IIoT Using PQC and Blockchain," *Comput. Commun.*, vol. 212, pp. 88–97, Mar. 2025.

[6] P. Agarwal, M. Bansal, and H. Kaushik, "Cross-Chain Supply Chain Management on IoT Blockchain," *Future Gener. Comput. Syst.*, vol. 153, pp. 709–721, Jan. 2024.

[7] L. Zhang and Q. Li, "Post-Quantum Blockchain Models for Embedded Devices," *Electronics*, vol. 13, no. 2, Feb. 2024.

[8] V. Bhatt and A. Chawla, "Resource Optimization in PQC for Edge IoT," *J. Netw. Comput. Appl.*, vol. 216, Jan. 2024.

[9] D. Nath and M. Verma, "Layer-2 Solutions in Interoperable IoT Blockchain Networks," *IEEE Commun. Surv. Tutor.*, early access, Mar. 2024.

[10] J. Mehta and K. Rana, "Hybrid PQC-Blockchain for Smart Metering," *IEEE Trans. Smart Grid*, vol. 15, no. 1, Feb. 2024.

[11] Y. Hossain, T. Gupta, and S. Roy, "Comparative Study of PQC for IoT Gateways," *Comput. Stand. Interfaces*, vol. 90, Apr. 2024.

[12] M. Sharma and L. Thomas, "Secure Identity Management Using Cross-Chain Ledgering," *Appl. Sci.*, vol. 14, no. 4, Apr. 2024.

[13] P. Singh and A. Goel, "Blockchain and PQC for Smart Agriculture Monitoring," *IEEE Trans. Ind. Informat.*, Mar. 2024.

[14] K. Reddy and T. Banerjee, "ZKP and PQC Convergence in IoT Authentication," *Inf. Secur. J.*, vol. 33, no. 1, Jan. 2024.

[15] R. Malhotra and I. Gupta, "A Review of Blockchain Interoperability in IoT Context," *J. Inf. Secur. Appl.*, vol. 78, Apr. 2024.

[16] B. D. Lee and J. Han, "Hash-Based PQC Framework for Edge IoT Devices," *IEEE Internet of Things Journal*, vol. 11, no. 4, pp. 2231–2244, Feb. 2024.

[17] T. Li, A. Joshi, and H. Phan, "Energy-Aware PQC-Blockchain Integration for IoT," *IEEE Access*, vol. 12, pp. 18635–18648, Mar. 2024.
[18] R. Kapoor and S. Patel, "Smart Contract Signing using Kyber in Ethereum," *ACM Trans. Cyber-Physical Syst.*, vol. 9, no. 1, Feb. 2024.
[19] A. Hussain, F. Ansari, and N. Mehra, "Interoperable Blockchain Bootloader for IoT Edge Devices," *IEEE Trans. Ind. Informat.*, vol. 20, no. 3, Jan. 2024.
[20] K. Verma and H. Rao, "Optimizing Cross-Chain IoT Communication," *Comput. Netw.*, vol. 234, pp. 109321, Mar. 2024.
[21] J. R. Thomas and P. Sahu, "Lattice-PKE in Permissioned Blockchain for Health Records," *IEEE Sensors Journal*, vol. 24, no. 6, Apr. 2024.
[22] S. Mishra and V. Sharma, "Hybrid Role-Based PQC Access Control for IIoT," *Springer IoT Journal*, vol. 21, no. 1, Jan. 2024.
[23] L. Anand, P. Nair, and R. Rathi, "PQC Migration Challenges in Smart Cities," *Appl. Sci.*, vol. 14, no. 2, Feb. 2024.
[24] F. Arora and M. Devraj, "Quantum-Secure Telemetry using Tendermint and Dilithium," *IEEE Trans. Veh. Technol.*, vol. 73, no. 2, Mar. 2024.
[25] H. Mehta and R. Ghosh, "Survey on PQC-Enabled Blockchain Frameworks," *Future Gener. Comput. Syst.*, vol. 158, pp. 281–298, Apr. 2024.