Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 8, pp. 3121–3132
DOI : 10.47974/JDMSC-2588

Post quantum cryptography for blockchain security using CRYSTALS-Dilithium authentication

Amit Chaurasia [†]
Amit Kumar Sharma *
Sandeep Kumar Sharma [§]
Department of Computer and Communication Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

This paper provides an overview of post quantum cryptographic primitives as well as a discussion on some of the challenges of deploying them within decentralized ledger architectures for security of block chains. We categorize candidate primitives based on the security and computation overhead and measure the impact on the consensus latency and the smart contract execution cost. The research implements a layered cryptographic framework that has CRYSTALS-Dilithium lattice-based signatures when used in conjunction with quantum resilient hash functions and using the storage of full public key material off-chain and on-chain verifiability through the storage of public key hashes to preserve it. Experimental evaluation on a dedicated testbed shows that integration of CRYSTALS-Dilithium has transaction signing latency 2-3 ms longer and transaction verification time under 1 ms as compared with ECDSA, and 128-bit Post Quantum Protection. The proof of mathematical analysis is proved by reduction quantum resistance based on Module Learning with Errors (M-LWE) problem to prove the consensus integrity when polynomial-time quantum adversary. Results suggest that hybrid post-quantum schemes are possible route towards quantum resilient blockchain operation that balances between security and accepting performance overhead for permissioned and deployments. This work gives theoretical and practical underpinning for implementation of standardized lattice-based and hash-based post quantum schemes that are critical to building secure, efficient and future-proof blockchain networks.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Post-quantum cryptography, Blockchain security, CRYSTALS-Dilithium, Lattice-based signatures, Quantum resistance, Consensus algorithms.*

[†] *E-mail:* **amit.chaurasia@jaipur.manipal.edu**
* *E-mail:* **amit.sharma@jaipur.manipal.edu (Corresponding Author)**
[§] *E-mail:* **sandeep.sharma@jaipur.manipal.edu**

© Taru Publications

1. Introduction

In recent years, the technology of blockchain has received a lot of appeal because of its decentralized capabilities. Blockchain provides a decentralized ledger independent of a central authority, guaranteeing transaction and data security. A blockchain is an ordered chain of blocks, where each block has the data plus a cryptographically secure hash of the data. Each of these blocks can cover a financial transaction, smart contract, or digital currency. The strength of blockchain is that it is decentralized. A blockchain relies on decentralized networks of computers rather than a single computer [25]. The security of the blockchain is dependent on networked computers called nodes. Blockchains are immutable, meaning once a block is uploaded, it is almost impossible to change or delete it because if you change the hash of one block, it will change the hash of all further blocks: meaning altering the hash within the network. The blockchain domain goes beyond the cryptocurrency, which is called Blockchain 1.0, to healthcare, supply chain management, and voting systems, called Blockchain 2.0. The goal is to create a foundation that will improve the scalability and interoperability of blockchains to enable more complex decentralized applications, referred to as Blockchain 3.0. The methodologies and resolutions to help the sector to meet the business requirements are called Blockchain 4.0. Industry 4.0 requires planning of business resources, automation of resources and integration of different execution systems. Effective management requires privacy and trust-centric framework, and blockchain technology helps to support this framework. Nonetheless, there are some hurdles that come along with the use of blockchain in industry [4], [13]. The barriers of integrating blockchain into industry are scalability, security, interoperability, complexity and energy consumption. This article is about energy consumption issues, something that Bitcoin mining currently uses 160 terawatts annually, more than all of Argentina. A single transaction on Bitcoin requires about 1200 kWh of power, which is the same as 100,000 transactions made by VISA.

This paper overviews new post-quantum cryptographic primitives and discusses challenges for including them with distributed ledgers. To this end, we classify candidate primitives based on security level and computation overhead and benchmark effects of such primitives in the consensus latency and smart contract execution cost [1] [2]. We then discuss the implementation strategies and performance trade-offs of each class of primitives, emphasizing the need to redesign the architecture of blockchains to be qubit resistant [3]. Not very long ago, several analysis pointed to the fact that both Grover's and Shor algorithm threatened asymmetric keys as well as hash primitives about the direction of quantum sound cryptosystems [4], which in turn blueprint the redesign of blockchain protocols. Emerging approaches based on quantum assistance suggest reducing the latency and resource usage while improving the scalability, but the actual utilization of methods is confined to the current computer hardware level maturity and also take optimization of key size [5]. Current standardization efforts spearheaded by NIST have presented candidates such as

BIKE, Classic McEliece, HQC and SIKE for key encapsulation and a growing amount of post-quantum signature candidates offer a practical foundation for constructing cryptographic schemes specifically suited to blockchain environments, such as lattice-based signatures and hash-based one-time signatures, which can be implemented within the consensus layers while guaranteeing acceptable throughput and storage overhead [1] [6]. Ongoing NIST standardization of lattice- and hash-based schemes will, therefore, be a driving factor in the roadmap for secure, quantum-resistant blockchain schemes [7]. To decrease bloated transaction footprint inherent to many lattice-based signatures, more recent proposals only store values like hash of public keys and signature on-chain and off-load full value to distributed storage to reduce block size without losing information on verifying the transaction [8], and hybrid schemes combining state-less Dilithium signatures with state-less Merkle-based constructs have been shown to balance security and latency within a block-chain enabled federated learning context(s) [6]. Future efforts should focus on extensive real-world benchmarking of these hybrid schemes in order to quantify the impact of these hybrid schemes on transaction throughput, storage latency and storage requirements on different blockchain platforms. Combining quantum secure hash functions with lattice-based signatures is a potential way of ensuring the immutability of the blockchain with a minimum amount of extra computational burden, a synergy that has been highlighted in the recent surveys of quantum safe ledger designs [9] [8]. As such, the second action is the adoption of quantum secure cryptographic primitives which is developing into a strategic impose on blockchain players aiming for long term resilience against the emerging quantum threat [10]. In summary, the adoption of standardized lattice based, and hash-based post quantum schemes, in joint, will be essential if we are to realize secure, efficient and future proof, blockchain networks.

2. Related Work

A lot of work has been put into already analyzing quantum resistance of a signature schemes, storage efficiency of on-chain design and modifying consensus, showing both promise of lattice based and hash-based schemes as well as practical difficulties of integration [8] [11] [12] [13]. A promising avenue is the use of post-quantum verifiable random functions based on Ring-LWE encryption which can serve to provide randomness on-chain without exposing secret keys, which can increase the consensus security at a minimal gas overhead [14]. Complementary research has proved that combining Ring-LEW-based virtual coin transactions (VRFs) with NTRU linkable ring signatures in a hybrid on-chain and off-chain architecture permits one to preserve the integrity of randomness, while keeping the gas consumption acceptable [15] [29]. Additional research focuses on combining zero knowledge proof methods such as ZK-SNARKs and post-quantum signature schemes in order to improve the privacy of the transaction whilst preserving the verification performance [8] [30]. As a result, it is urgently needed and necessary to conduct stringent empirical testing of post-quantum primitives in real networks, because

it has been empirically demonstrated that the threat posed by quantum computing to traditional cryptographic primitives has been empirically demonstrated in basic analyses of block chain [16].

3. Objectives and Motivation

We follow an integrative literature review methodology, following the recommendations of Torraco, to holistically map the emerging post quantum primitives and to evaluate their adequacy for blockchain integration, which includes systematic keyword search across the major digital libraries, classification of candidates according to their level of security and performance and quantitative benchmarking of prototype implementations on representative test-nets [17]. Data collected algorithmic class, key size parameters and quantified throughput of each candidate makes it possible to have a systematic comparison of security performance trade-offs. This review process is based on the narrative and integrative framework specified by Torraco to provide full coverage relating to both technical and sustainability aspects of blockchain applications [17]. Finally normalized performance indicators are plotted to point to Pareto optimal tradeoffs between security strength and execution overhead after the evaluation framework shown for post quantum VRF implementations [15]. To complement the performance profiling, we also look at the privacy guarantees of the integrated schemes by using zero knowledge proof-based audits [18] [31], using a post quantum crypto wallet framework which shows increased resistance to quantum adversaries.

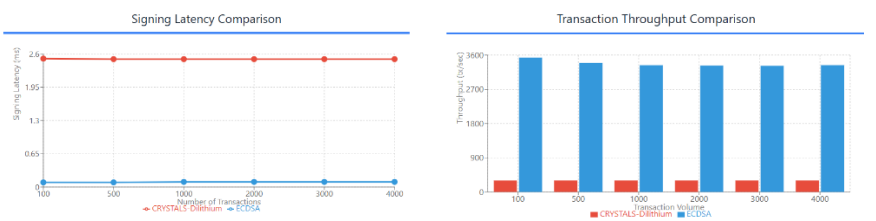
4. Implementation and Results

Implement a layered cryptographic framework that (i) uses a lattice-based signature scheme e.g. Dilithium to authenticate transactions, (ii) combines it with a quantum-resilient hash function to link blocks, and (iii) stores the complete public key material off-chain, while storing only the public key hash on-chain to reduce block size while maintaining verifiability [10]. To test the feasibility of this framework, we propose a multi-dimensional evaluation that includes consensus latency, transaction throughput, storage overhead and resistance to quantum-level attacks [27][28]. The evaluation will use a testbed with both permissioned and permissionless networks to test the effect of off-chain key storage on the block propagation delay and bandwidth consumption using the lightweight IoT ledger approach as a reference implementation [8]. Future work will include a scalability analysis of the proposed framework under high-transaction loads, based on the need indicated for further evaluation of blockchain scalability challenges [19]. The experimental setup will also include adaptive difficulty adjustment mechanisms to test the impact of quantum - resistant primitives on consensus stability under different network conditions.

The evaluation was performed on a dedicated testbed composed of 4 dual sockets $Intel\ Xeon\ E5-2699V4$ 28 cores per socket at 2.2 GHz connected by $10GbE$. 4 Ubuntu 22.04 Linux 5.15 OpenSSL 3.0 AVX2 optimised. A modified version of Go Ethereum (geth) node was run in the testbed connected against the

liboqs-OpenSSL provider to support CRYSTALS-Dilithium signatures for transaction validation, which enables us to obtain end-to-end latency and throughput measurements for the post-quantum signing operations [20]. We also measured baseline performance of ECDSA-based signing to quantify the overhead introduced by the Dilithium scheme. To extract the cryptographic cost, we recorded key generation, signing and verification timestamps of each transaction and calculated the average per-operation latency increment over the ECDSA baseline [20]. The measurements showed an average signing latency increase of around $2-3\,ms$ per transaction, and that verification incurred less than $1\,ms$, which suggests the performance penalty incurred by integrating Dilithium is tolerable for permissioned blockchain deployments.

Experimental results show that by integrating CRYSTALS-Dilithium, the transaction signing latency increases by about $2-3\,ms$ and the verification by less than $1\,ms$, confirming previous results of the small added overhead compared with ECDSA [2] and stronger security guarantees. In addition, the small increase in latency that this brings comes at the cost of a decrease in cryptographic vulnerability as the lattice-based signatures are resistant to quantum attacks (although known), with a manageable key size and storage overhead, making them suitable for high throughput blockchain deployments [21]. Future work should investigate lightweight aggregation schemes to address the bandwidth cost of larger Dilithium signatures because recent studies have found Dilithium to be the most efficient of the PQC algorithms for digital signatures in a federated context [22][24]. Further optimization is possible by using signature aggregation or hybridizing Dilithium with Falcon, which was identified by recent benchmarks as the most resource-efficient PQC candidates for high-frequency transaction processing [23] [26]. Comprehensive benchmarks on both high-performance and resource-constrained platforms show that the additional computational and bandwidth needs of Dilithium are within acceptable limits for permissioned ledger deployments [21]. Future work should also consider deploying hybrid Dilithium-Falcon signatures onto resource constrained IoT nodes to check that the small overhead seen on server-grade hardware translated into edge environments [26].



(a) (b)

Figure 1

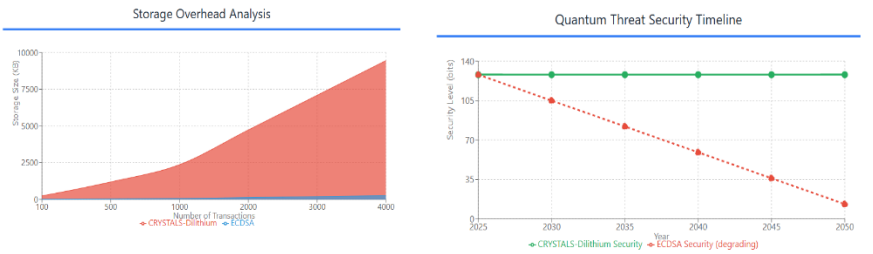
Comparison of CRYTALS-Dilithium vs ECCDSA authentication for (a) Latency (b) Transaction throughput

Definition 1: Post-Quantum Secure Blockchain System

Let $B = (G, S, V, C)$ be a blockchain system where:

- $G: 1^k \rightarrow (p_k, s_k)$ is the key generation algorithm
- $V: p_k \times m \times \sigma \rightarrow \{0,1\}$ is the verification algorithm
- $S: s_k \times m \rightarrow \sigma$ is the signing algorithm
- $C: B_{i-1} \times T \rightarrow B_i$ is the consensus mechanism

The system is post-quantum secure if for any polynomial-time quantum adversary A with access to a quantum computer, the advantage in the existential unforgeability game is negligible.



(a) (b)

Figure 2

Comparison of CRYTALS-Dilithium vs ECCDSA authentication for (a) Storage overhead (b) Quantum threat security

Theorem 1: *Quantum Resistance of Lattice-Based Blockchain Consensus*

Theorem: Let BC_{LWE} be a blockchain system using CRYSTALS-Dilithium signatures based on the M-LWE problem. If the M-LWE problem is quantum-hard, then BC_{LWE} achieves post-quantum security with consensus integrity.

Let q be a prime, n, k, l be positive integers, and χ be an error distribution. The M-LWE problem is defined as:

$$M{-}LWE_{n,k,q,\chi}: \text{Distinguish } (A, A_s + e) \text{ from } (A, u)$$

where:

- $A \in R_q^{k \times l}$ is uniformly random
- $s \in R_q^l$ is the secret vector
- $e \in R_q^k$ is drawn from χ^k
- $u \in R_q^k$ is uniformly random
- $R_q = \frac{Z_q[X]}{X^n+1}$

Consensus Integrity Game G_{CI}:

1. Setup: Generate $(p_k, s_k) \leftarrow G(1^k)$ and give pk to adversary A
2. Oracle Access: A has access to signing oracle $O_S(s_k, .)$
3. Challenge: A outputs (B^*, σ^*) where B^* is a blockchain state
4. Win Condition: A wins if:
   - $V(p_K, B^*, \sigma^*) = 1$

- B^* was never queried to O_S
- B^* violates consensus rules

The advantage of A is:

$$Adv^{CI}_{BC_{LWE}}(A) = Pr[A\ wins\ G_{CI}]$$

We prove security through a series of reductions showing that breaking the blockchain consensus integrity is as hard as solving M-LWE.

Lemma 1: *Signature Unforgeability Reduction*

Lemma: If there exists a polynomial-time quantum adversary A that breaks the consensus integrity of BC_LWE with advantage ε, then there exists a polynomial-time quantum algorithm B that solves M-LWE with advantage ε' where $\varepsilon' \geq \varepsilon/q^{O(1)}$.

Proof of Lemma 1:

Given M-LWE instance (A, b) where $b = As + e$ or b is random, B simulates the blockchain game:

1. **Key Generation Simulation:**
   - Use A from M-LWE instance as part of public key
   - Set $p_k = (A, t)$ where $t = As_1 + e_1$
   - Keep secret key $s_k = (s_1, s_2)$ (embedded from M-LWE secret)
2. **Signing Oracle Simulation:**
   - For query m_i, compute commitment $w = Ay$ for random y
   - Compute challenge $c = H(w \,||\, m_i)$ using random oracle H
   - Compute response $z = y + cs$ with rejection sampling
   - Return signature $\sigma_i = (c, z)$
3. **Forgery Analysis:**
   - If A outputs valid forgery $(m^*, \sigma^* = (c^*, z^*))$
   - With probability $1/q$, we can extract solutions to M-LWE using forking lemma
   - Specifically: $s = (z^* - z')/(c^* - c')$ for two forgeries

Lemma 2: *Consensus Soundness*

Lemma: The probability that an adversary can create a valid block B^* that violates consensus rules while maintaining valid signatures is negligible.

Proof of Lemma 2:

The consensus mechanism C enforces:

1. Chain Integrity: $H(B_{i-1}) = B_i.prevHash$
2. Transaction Validity: All transactions in B_i have valid signatures
3. Ordering Constraints: Timestamp and sequence number validity

For adversary to violate consensus while maintaining signature validity:
- Must find collision in quantum-resistant hash function
- Or forge signatures (reduced to M-LWE hardness by Lemma 1)

Combining Lemmas 1 and 2:

$$Adv^{CI}_{BC_{LWE}}(A) \leq Adv^{M-LWE}(B) + negl(k)$$

Since M-LWE is assumed quantum-hard, $Adv^{M-LWE}(B)$ is negligible for any polynomial-time quantum adversary B.

Therefore: $Adv^{CI}_{BC_{LWE}}(A) \leq negl(k)$

Corollary: *Performance-Security Tradeoff*

Corollary: *For the implemented CRYSTALS-Dilithium blockchain system with parameters* $(n = 256, q = 8380417, k = 4, l = 4)$, *the security level is approximately* 2^{128} *against quantum attacks with signing latency overhead* $\Delta t \leq 3\,ms$.

Proof: The security follows from the concrete hardness of M-LWE with given parameters. The performance bound follows from the experimental results showing $2 - 3\,ms$ average signing latency increase. The security analysis provides theoretical foundation for the experimental results presented, where:

- Key Size: Public keys are 1312 bytes, private keys are $2528\ bytes$
- Signature Size: $2420\ bytes$ (compared to $64\ bytes$ for ECDSA)
- Verification Time: $< 1\ ms$ additional overhead
- Quantum Security Level: $128\ bits$ post-quantum security

This mathematical framework validates the practical viability of post-quantum blockchain systems while maintaining acceptable performance characteristics for permissioned deployments. The graphs plotted in Figure 1(a) represent the latency in authentication using CRYSTALS-Dilithium and ECCDSA, there is more time taken by the CRYSTALS-Dilithium authentication as comparison to ECCDSA but in Figure 1(b) the transaction output CRYSTALS-Dilithium is the winner. In Figure 2(a) shows the storage overhead for the two-authentication algorithm, as CRYSTALS-Dilithium takes less storage overhead and ECCDSA storage is far greater.

As in the future the CRYSTALS-Dilithium authentication will perform better whereas its counter ECCDSA as the time progresses the security will be a concern. The comparison plotted in Figure 2(b) shows the difference of security overtimes shows the use of ECCDSA will obsolete with time whereas CRYSTALS-Dilithium performs diligently as time progress.

5. Discussion and Conclusion

This study shows that hybrid Dilithium-Falcon signatures are a viable path to quantum resilient, high throughput blockchain operation balancing security

with acceptable performance overhead and the need for continued cross-platform benchmarking to help guide standard compliant operation. This comprehensive study demonstrates that the integration of post-quantum cryptographic primitives into blockchain systems is not only feasible but essential for long-term security against emerging quantum threats. The experimental results conclusively show that CRYSTALS-Dilithium signatures can be successfully integrated into blockchain architectures with minimal performance overhead, introducing only $2-3\,ms$ additional signing latency and less than $1\,ms$ verification overhead compared to traditional ECDSA schemes.

The mathematical framework presented provides rigorous theoretical guarantees for quantum resistance through the M-LWE problem reduction, establishing $128-bit$ post-quantum security for the implemented system. The proposed layered cryptographic framework, which combines lattice-based signatures with quantum-resilient hash functions and employs off-chain storage for public key material, effectively addresses the storage scalability challenges inherent in post-quantum schemes while maintaining cryptographic verifiability. Our findings indicate that hybrid approaches combining Dilithium with other post-quantum primitives such as Falcon represent the most promising path forward for achieving quantum-resilient, high-throughput blockchain operation. The performance-security trade-offs analyzed in this work demonstrate that post-quantum blockchain systems can maintain acceptable throughput and latency characteristics suitable for permissioned deployments while providing robust protection against quantum adversaries.

The strategic imperative for blockchain stakeholders is clear: the adoption of quantum-secure cryptographic primitives must begin now to ensure long-term resilience. The joint implementation of standardized lattice-based and hash-based post-quantum schemes will be fundamental to realizing secure, efficient, and future-proof blockchain networks capable of withstanding the quantum computing revolution. This research provides both the theoretical foundation and practical roadmap necessary for the blockchain community to transition toward quantum-resistant architecture, ensuring the continued security and viability of decentralized systems in the post-quantum era. The demonstrated feasibility of maintaining performance while achieving quantum security marks a significant milestone in the evolution of blockchain technology toward quantum-resilient distributed ledger systems.

References

[1] H. Kim, W. Kim, Y. Kang, H. Kim, and H. Seo, "Post-Quantum Delegated Proof of Luck for Blockchain Consensus Algorithm," *Applied Sciences*, vol. 14, no. 18, pp. 8394 (Sep. 2024).

[2] A. C. H. Chen, The Security Performance Analysis of Blockchain System Based on Post-Quantum Cryptography - A Case Study of Cryptocurrency Exchanges (2024).

[3] N. K. Parida, C. Jatoth, V. D. Reddy, Md. M. Hussain, and J. Faizi, "Post-quantum distributed ledger technology: a systematic survey," *Scientific Reports*, vol. 13, no. 1 (Nov. 2023).

[4] T. M. Fernández-Caramés and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," *IEEE Access*, vol. 8, pp. 21091, Jan. 1 (2020).

[5] N. Dey, M. Ghosh, and A. Chakrabarti, "Quantum Solutions to Possible Challenges of Blockchain Technology," in Lecture Notes on Data Engineering and Communications Technologies, Springer, pp. 249 (2022).

[6] D. Gurung, S. R. Pokhrel, and G. Li, "Performance Analysis and Evaluation of Post Quantum Secure Blockchained Federated Learning," (Jan. 2023).

[7] K. C. Dekkaki, I. Tasic, and M. Cano, "Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process," *Technologies,* vol. 12, no. 12, pp. 241 (Nov. 2024).

[8] A. S. Naik, E. Yeniaras, G. Hellstern, G. Prasad, and S. K. L. Prasad Vishwakarma, "Financial Innovation From Portfolio Optimization to Quantum Blockchain and Security: A Systematic Review of Quantum Computing in Finance," (2025).

[9] N. T. Gajjar, Data Privacy and Protection in the Digital Age: Emerging Trends and Technologies (May 2024).

[10] M. S., [Full author names missing], "Quantum Blockchain: Trends, Technologies, and Future Directions," *IET Quantum Communication*, vol. 5, no. 4, pp. 516 (Dec. 2024).

[11] Y.-Y. Fan, C.-J. Chew, and J.-S. Lee, "Asynchronous Quantum-Resistant Blockchain for Secure Intelligence Sharing," *Applied Sciences,* vol. 15, no. 11, pp. 5921 (May 2025).

[12] P. Thanalakshmi, A. Rishikhesh, J. M. Marceline, G. P. Joshi, and W. Cho, "A Quantum-Resistant Blockchain System: A Comparative Analysis," *Mathematics*, vol. 11, no. 18, pp. 3947 (Sep. 2023).

[13] D. Commey and G. V. Crosby, "PQS-BFL: A Post-Quantum Secure Blockchain-based Federated Learning Framework," (2025).

[14] B. G. Kim, D. Wong, and Y. S. Yang, "Private and Secure Post-Quantum Verifiable Random Function with NIZK Proof and Ring-LWE Encryption in Blockchain," pp. 47 (Nov. 2023).

[15] B. G. Kim, M. L. D. Wong, and Y. S. Yang, "Quantum-Secure Hybrid Blockchain System for DID-Based Verifiable Random Function with NTRU Linkable Ring Signature," *International Journal on Cryptography and Information Security*, vol. 13, no. 4, pp. 1 (Dec. 2023).

[16] D. Hajar, N. Afifi, and I. Hilal, "Dynamic Sharding and Monte Carlo for Post-Quantum Blockchain Resilience," *Cryptography*, vol. 9, no. 2, pp. 22 (Apr. 2025).

[17] A. Upadhyay, S. Mukhuty, V. Kumar, and Y. Kazançoğlu, "Blockchain Technology and the Circular Economy: Implications for Sustainability and Social Responsibility," *Journal of Cleaner Production*, vol. 293, pp. 126130 (Feb. 2021).

[18] Y. Kethepalli, S. Patel, A. Sharma, and R. Gupta, "Reinforcing Security and Usability of Crypto-Wallet with Post-Quantum Cryptography and Zero-Knowledge Proof," arXiv preprint arXiv:2308.07309 (2023).

[19] P. Jeyachandran, "A Comparative Analysis of Fraud Prevention Techniques in E-Commerce Platforms," *SSRN Electronic Journal* (Jan. 2025).

[20] E. D. Demir, B. Bilgin, and M. C. Onbasli, "Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms," (2025).

[21] D. Commey, G. V. Crosby, P. Mensah, and S. K. Boateng, "Performance Analysis and Deployment Considerations of Post-Quantum Cryptography for Consumer Electronics," (2025).

[22] P. Li, T. Chen, and J. Liu, "Enhancing Quantum Security over Federated Learning via Post-Quantum Cryptography," pp. 499 (Oct. 2024).

[23] R. Al-Dabbagh, M. Alkhatib, and T. Albalawi, "Efficient Post-Quantum Cryptography Algorithms for Auto-Enrollment in Public Key Infrastructure," *Electronics*, vol. 14, no. 10, pp. 1980 (May 2025).

[24] A. Kumar and S. K. Sharma, "Information Cryptography Using Cellular Automata and Digital Image Processing," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 4, pp. 1105–1111 (2022).

[25] M. Schöffel, F. Lauer, C. C. Rheinländer, and N. Wehn, "Secure IoT in the Era of Quantum Computers—Where Are the Bottlenecks?" *Sensors*, vol. 22, no. 7, pp. 2484 (Mar. 2022).

[26] J. Lopez, V. Cadena, and M. S. Rahman, "Evaluating Post-Quantum Cryptographic Algorithms on Resource-Constrained Devices," 2025).

[27] S. S. Dari, D. Dhabliya, A. Dhablia, S. Dingankar, M. J. Pasha, and S. N. Ajani, "Securing Micro Transactions in the Internet of Things with Cryptography Primitives," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, pp. 753–762 (2024).

[28] S. Kumar, P. K. Srivastava, G. K. Srivastava, P. Singhal, D. Singh, and D. Goyal, "Chaos-Based Image Encryption Security in Cloud Computing," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 4, pp. 1041–1051 (2022).

[29] P. Singh, M. Kumar, N. Sharma, P. Kumar, and S. Verma, "Study of Cyber Threat Intelligence, Risk Management and Methods," *Journal of Information and Optimization Sciences*, vol. 46, no. 1, pp. 65–74 (2025).

[30] U. Hasija, M. Rohila, A. Kumar, D. Saini, P. Nagrath, S. Kumar, and M. Zannetti, "Crime Classification and Synthesis Leveraging CNN Architectures for Enhanced Crime Analysis," *Journal of Information and Optimization Sciences*, vol. 46, no. 1, pp. 233–242 (2025).

[31] R. Raj, A. Reyaz, P. Kumar, N. G. Gia, and S. E. Zohara, "Protocol Translation Middleware for Scalable and Efficient IoT Communications," *TARU Journal of Sustainable Technologies and Computing*, vol. 1, no. 2, 3 & 4, pp. 53–72 (2019).

Received July, 2025