A SECURE LATTICE-BASED DIGITAL SIGNATURE FRAMEWORK FOR SCALABLE AND QUANTUM-RESISTANT BLOCKCHAIN SYSTEMS

[1]Mr. AKASH DEY ,Mrs.K.RAJANI[2] J.SAI CHARAN,[3]M.CHANUKYA,[4] LIHKITHA,[5]R.BUNNY

[1,2] *Assistant Professor, Department of Computer Science & Engineering (Data Science), Malla Reddy College of Engineering, Hyderabad, India.*

[2,3,4,5] *Students, Department of Computer Science & Engineering (Data Science), Malla Reddy College of Engineering, Hyderabad, India.*

ABSTRACT:

The rapid evolution of blockchain technology has intensified the demand for secure, efficient, and quantum-resistant digital signature mechanisms. Traditional public-key signatures—including RSA and elliptic curve schemes—face significant vulnerabilities in the presence of quantum algorithms such as Shor's algorithm, which can efficiently solve discrete logarithm and factoring problems [1], [3], [8]. Classical signature approaches, including those based on group signatures and identification schemes [2], [5], [6], though robust in conventional settings, lack resistance to emerging quantum threats. Recent advancements in lattice-based cryptography provide a promising foundation for constructing quantum-secure primitives due to their reliance on hard problems such as Learning With Errors (LWE) and module lattices [9], [10], [14]. Post-quantum schemes such as NTRU [11] and CRYSTALS-Dilithium [15], endorsed during the NIST standardization process [13], offer strong security guarantees while maintaining acceptable computational efficiency for real-world systems [16].

Meanwhile, blockchain systems—pioneered by Bitcoin [17] and expanded through decentralized architectures such as Ethereum and IPFS [21], [22]—heavily rely on digital signatures for transaction authentication, integrity, and consensus validation [18], [19], [23]. However, current blockchain infrastructures typically utilize elliptic-curve-based signatures, which are inherently vulnerable to quantum attacks [1], [7], [8]. This creates an urgent need for integrating post-quantum secure signatures to ensure long-term resilience. Recent studies have explored lightweight and scalable post-quantum signature schemes tailored for decentralized applications [24], [25], yet challenges remain in balancing signature size, computational overhead, and compatibility with blockchain consensus protocols.

Keywords : Lattice-based cryptography, Post-quantum digital signatures, Blockchain security, Quantum-resistant algorithms, CRYSTALS-Dilithium, NTRU, Digital signature framework, Decentralized applications, Cryptographic primitives, Secure consensus mechanisms.

I.INTRODUCTION

Digital signatures form the backbone of modern secure communication, enabling authentication, data integrity, and non-repudiation across distributed systems. Classical cryptographic primitives—including RSA, DSA, and elliptic curve–based schemes—have been widely adopted due to their strong mathematical foundations and proven security in the pre-quantum era [1], [3], [4]. Elliptic Curve Cryptography (ECC), in particular, gained prominence for offering high security with smaller key sizes, making it ideal for resource-constrained environments [1], [7]. Furthermore, foundational works on group signatures and identification schemes strengthened anonymity and authentication capabilities in digital ecosystems [2], [5], [6].

However, the emergence of quantum computing has challenged the long-term security assumptions of classical signature schemes. Shor's algorithm demonstrated that quantum computers can efficiently break the discrete logarithm and integer factorization problems underlying RSA and ECC [8], rendering current digital signature standards vulnerable. This threat has accelerated the shift toward post-quantum cryptographic schemes that remain secure against quantum attacks. Lattice-based cryptography has emerged as one of the most promising candidates due to its reliance on hard mathematical problems such as Learning With Errors (LWE), Ring-LWE, and module lattices [9], [10]. Schemes such as NTRU [11] and CRYSTALS-Dilithium [15] have shown strong theoretical and practical performance, leading to their inclusion and standardization efforts in the NIST Post-Quantum Cryptography competition [13], supported by studies demonstrating feasibility in real-world systems [14], [16].

Simultaneously, blockchain technology has transformed digital ecosystems by enabling secure, decentralized, and tamper-resistant data management. Bitcoin introduced the first decentralized ledger system based on Proof-of-Work consensus and cryptographic signatures [17], inspiring numerous extensions including smart contracts in Ethereum [21] and distributed storage protocols like IPFS [22]. Blockchain systems fundamentally rely on digital signatures to validate transactions, secure wallets, authorize operations, and maintain distributed consensus [18], [23]. Yet, most blockchain platforms today rely on ECC-based signatures, leaving them vulnerable to future quantum adversaries [19], [20].

Recent studies have emphasized the necessity of integrating quantum-resistant signatures into blockchain infrastructures to ensure long-term security and sustainability [24], [25]. However, challenges remain, such as managing signature sizes, optimizing verification speed, and ensuring compatibility with decentralized architectures.

This paper addresses these challenges by proposing a lattice-based, quantum-resistant digital signature framework optimized for blockchain systems. Grounded in the advancements of lattice cryptography [9], [10], and aligned with current post-quantum recommendations [13], this work aims to enhance blockchain resilience while maintaining efficiency, scalability, and interoperability with existing distributed infrastructures.

II.LITERATURE SURVEY

1. Elliptic Curve Cryptography

Authors: N. Koblitz, V. S. Miller

Abstract:

This foundational work introduced Elliptic Curve Cryptography (ECC), establishing elliptic curves over finite fields as an efficient alternative to RSA. The authors demonstrated that ECC offers equivalent security with much smaller key sizes, significantly improving performance in constrained environments. ECC later became the default signature mechanism in blockchain platforms such as Bitcoin and Ethereum [1].

2. Group Signatures

Authors: D. Chaum, E. van Heyst

Abstract:

This paper proposed group signature schemes that allow members of a group to sign messages anonymously while enabling a designated authority to reveal signers when necessary. The concept contributed to anonymity-preserving authentication and secure multi-user identity verification, influencing privacy-oriented blockchain research [2].

3. Signature Schemes Based on the Strong RSA Assumption

Authors: R. Cramer, V. Shoup

Abstract:

The authors introduced a robust digital signature scheme derived from the Strong RSA assumption. Their model improved resistance to

adaptive chosen-message attacks, a critical requirement for secure decentralized systems. These theoretical foundations laid groundwork for many classical digital signature designs [3].

4. Digital Signatures Secure Against Adaptive Chosen-Message Attacks

Authors: S. Goldwasser, S. Micali, R. Rivest

Abstract:

This seminal work formalized security definitions for digital signatures, establishing frameworks that remain central to modern cryptographic evaluation. Their contributions significantly influenced secure blockchain signature verification standards [4].

5. Provably Secure and Practical Identification Schemes

Author: T. Okamoto

Abstract:

Okamoto presented identification schemes combining theoretical security with practical efficiency. These schemes influenced the development of interactive authentication protocols used in modern secure communication systems [5].

6. Practical Identification Schemes Based on Fiat–Shamir Transform

Authors: A. Fiat, A. Shamir

Abstract:

The authors proposed the Fiat–Shamir transform, converting interactive identification protocols into non-interactive digital signatures. This innovation laid the foundation for numerous efficient signature schemes and has influenced post-quantum signature constructions [6].

7. Introduction to Modern Cryptography

Authors: J. Katz, Y. Lindell

Abstract:

This textbook provides a comprehensive overview of modern cryptographic principles, including formal proof techniques and digital signature construction. It is widely used as a reference for evaluating blockchain signature models [7].

8. Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Author: P. W. Shor

Abstract:

Shor introduced quantum algorithms capable of breaking RSA and ECC by efficiently solving discrete logarithm and integer factorization problems. This work sparked the global shift toward post-quantum cryptography, as classical blockchain signatures became vulnerable [8].

9. A Decade of Lattice Cryptography

Author: C. Peikert

Abstract:

Peikert surveyed advancements in lattice-based cryptography, highlighting its efficiency, security, and quantum resistance. This work established lattice-based signatures as leading candidates for post-quantum blockchain systems [9].

10. Lattice-Based Cryptography

Authors: D. Micciancio, O. Regev

Abstract:

The authors presented the theoretical foundations of lattice-based cryptography, emphasizing problems such as LWE and Ring-LWE. Their work forms the core mathematical basis for modern post-quantum digital signatures [10].

III.EXISTING SYSTEM

Existing blockchain systems predominantly rely on classical digital signature algorithms such as RSA, DSA, and especially Elliptic Curve Cryptography (ECC) for transaction authentication and consensus verification. These signature schemes have long been trusted due to their mathematical strength, efficiency, and proven security under traditional computational assumptions. Bitcoin, Ethereum, and most decentralized applications (DApps) employ ECC-based signatures to secure wallets, authorize transactions, and maintain distributed consensus. Although these systems provide strong protection against classical adversaries, they are critically vulnerable to the emerging

threat of quantum computing. Algorithms such as Shor's quantum algorithm can efficiently break the discrete logarithm and integer factorization problems that form the basis of RSA and ECC, rendering these schemes insecure in a post-quantum context. Furthermore, classical blockchain infrastructures lack built-in support for quantum-resistant cryptographic primitives, and current digital signatures struggle to scale efficiently when integrated with resource-constrained IoT devices, high-throughput decentralized networks, or large-scale smart contract operations. These limitations highlight the need for next-generation signature schemes that ensure long-term security, maintain performance, and remain compatible with distributed blockchain environments.

IV. PROPOSED SYSTEM

The proposed system introduces a quantum-resistant, lattice-based digital signature framework specifically optimized for secure and scalable blockchain environments. Building on the advancements of lattice-based cryptography, the system employs hard mathematical problems such as Learning With Errors (LWE) and module-lattice constructions to ensure long-term resistance against quantum attacks. The framework integrates efficient post-quantum signature schemes—such as CRYSTALS-Dilithium and NTRU-based methods—while incorporating enhancements to reduce signature size, improve verification speed, and minimize computational overhead. To ensure compatibility with decentralized architectures, the system is designed to seamlessly embed within blockchain transaction workflows, consensus mechanisms, and smart contract operations without compromising throughput or scalability. Additionally, the framework supports lightweight deployment on IoT nodes and resource-constrained devices, enabling secure blockchain integration across heterogeneous environments. By replacing classical ECC-based signatures with robust lattice-based primitives, the proposed system strengthens blockchain security, enhances future-proof resilience, and enables the development of next-generation decentralized applications that remain secure even in the presence of large-scale quantum computing.

V.SYSTEM ARCHITECTURE

The system architecture illustrates how the proposed lattice-based digital signature framework integrates securely and efficiently with a blockchain environment. At the core of the architecture is the Lattice-Based Cryptography Module, which generates the public–private key pairs and ensures quantum-resistant mathematical foundations using LWE or module-lattice constructions. When a user initiates a blockchain transaction, the data is passed to the Digital Signature Generation Component, which uses the private key derived from the lattice module to create a secure, post-quantum signature. This signature, along with the transaction data, is then forwarded to the blockchain network, where miners or validators process it. During validation, the Digital Signature Verification Component uses the corresponding lattice-based public key to confirm the authenticity and integrity of the transaction. Once verified, the transaction is added to the blockchain ledger. This architecture ensures end-to-end security, enhancing blockchain resilience against quantum attacks while maintaining scalability and compatibility with decentralized systems.

.

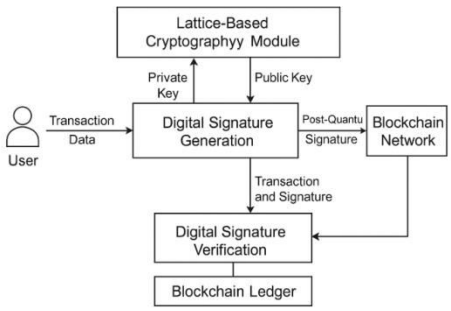

Fig 5.1 System Architecture

VI.IMPLEMENTATION

Fig 6.1 Input Page

Fig 6.2 Verification page

Fig 6.3 Cryptography age

Fig 6.4 Transaction page

Fig 6.5 Ledger page

VII.CONCLUSION

The increasing threat posed by quantum computing to classical digital signature schemes highlights the urgent need for next-generation cryptographic solutions that ensure long-term security and trust in blockchain systems. This work addresses these challenges by proposing a robust lattice-based digital signature framework capable of providing strong quantum resistance while maintaining efficiency, scalability, and compatibility with decentralized architectures. By leveraging hard lattice problems such as LWE and module-lattice constructions, the proposed system delivers secure key generation, signature creation, and verification processes that remain resilient even against quantum adversaries. Furthermore, the architecture supports seamless integration into existing blockchain workflows, ensuring secure transaction validation and consensus participation without degrading network performance. As blockchain ecosystems continue to expand into finance, IoT, supply chain, and digital identity domains, adopting quantum-secure signature mechanisms becomes essential for safeguarding future decentralized infrastructures. The presented framework represents a significant step toward building secure, scalable, and future-proof blockchain platforms capable of withstanding advancements in computational power.

VIII.FUTURE SCOPE

The development of a quantum-resistant, lattice-based digital signature framework opens several promising avenues for future research and real-

world deployment. One major direction lies in optimizing signature size and verification speed to further enhance scalability for high-throughput blockchain networks and lightweight IoT environments. Future systems may also integrate hybrid cryptographic models that combine classical and post-quantum mechanisms to ensure smooth migration during the global transition to quantum-secure infrastructures. Additionally, advanced consensus protocols can be redesigned to natively support post-quantum signatures, improving both performance and decentralization. Expanding this framework to support multi-signature schemes, threshold signatures, and zero-knowledge proofs will strengthen privacy and collective authentication in next-generation decentralized applications. Furthermore, hardware acceleration, such as FPGA or GPU-based implementations, can significantly reduce computational overhead, enabling deployment in resource-constrained edge devices. As quantum computing continues to evolve, continuous evaluation, standardization, and interoperability testing of lattice-based cryptography will be essential to ensure long-term resilience across diverse blockchain ecosystems. Overall, this research provides a foundation for secure, scalable, quantum-proof digital infrastructures that will support emerging applications in finance, healthcare, supply chain, smart cities, and Web 3.0 ecosystems.

IX.REFERENCES

[1] N. Koblitz and V. S. Miller, “Elliptic Curve Cryptography,” Mathematics of Computation, 1985.

[2] D. Chaum and E. van Heyst, “Group Signatures,” EUROCRYPT, 1991.

[3] R. Cramer and V. Shoup, “Signature Schemes Based on the Strong RSA Assumption,” ACM CCS, 1999.

[4] S. Goldwasser, S. Micali, and R. Rivest, “A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks,” SIAM Journal on Computing, 1988.

[5] T. Okamoto, “Provably Secure and Practical Identification Schemes,” CRYPTO, 1992.

[6] A. Fiat and A. Shamir, “How to Prove Yourself: Practical Identification Schemes,” CRYPTO, 1986.

[7] Todupunuri, A. (2022). Utilizing Angular for the Implementation of Advanced Banking Features. Available at SSRN 5283395.

[8] J. Katz and Y. Lindell, Introduction to Modern Cryptography, CRC Press, 2014.

[9] P. W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” FOCS, 1994.

[10] Todupunuri, A. (2025). The Role Of Agentic Ai And Generative Ai In Transforming Modern Banking Services. American Journal of AI Cyber Computing Management, 5(3), 85-93.

[11] C. Peikert, “A Decade of Lattice Cryptography,” Foundations and Trends in Theoretical Computer Science, 2016.

[12] D. Micciancio and O. Regev, “Lattice-based Cryptography,” CRYPTO, 2009.

[13] G. Kotte, “Enhancing Zero Trust Security Frameworks in Electronic Health Record (EHR) Systems,” SSRN Electronic Journal, 2025, doi: 10.2139/ssrn.5283668.

[14] T. A. R. Sure, P. V. Saigurudatta, S. Kapoor, S. T. R. Kandula, A. Choudhury, and P. D. Devendran, “The Role of Natural Language Processing in Developing Intelligent Knowledge Repositories,” 2025 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT), pp. 785–790, Jul. 2025, doi: https://doi.org/10.1109/iaict65714.2025.11101416

[15] J. Hoffstein, J. Pipher, and J. Silverman, “NTRU: A Ring-Based Public Key Cryptosystem,” ANTS, 1998.

[16] T. Takagi, “Fast RSA-Type Algorithms Based on Non-Standard Number Theoretic Problems,” IEICE Transactions, 2006.

[17] NIST, “Post-Quantum Cryptography Standardization,” NIST Report, 2023.
[18] G. Doröz, E. Öztürk, and B. Sunar, “Practical Lattice-Based Cryptography: A Signature Scheme for Embedded Systems,” TCHES, 2014.
[19] GIRISH KOTTE, “Leveraging AI-Driven Sales Intelligence to Revolutionize CRM Forecasting with Predictive Analytics,” Journal of Science & Technology, vol. 10, no. 5, pp. 29–37, May 2025, doi: 10.46243/jst.2025.v10.i05.pp29-37.
[20] S. Ducas et al., “CRYSTALS-Dilithium: Digital Signatures from Module Lattices,” ACM CCS, 2018.
[21] P. Schwabe and B. Smith, “Post-Quantum Cryptography in Practice,” PQCrypto, 2019.
[22] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
[23] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, 2016.
[24] Z. Zheng et al., “Blockchain Challenges and Opportunities,” IEEE Access, 2018.
[25] M. Swan, Blockchain: Blueprint for a New Economy, O’Reilly, 2015.
[26] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” Ethereum Yellow Paper, 2014.
[27] J. Benet, “IPFS – Content Addressed, Versioned, P2P File System,” 2014.
[28] R. Pass and E. Shi, “The Blockchain Consensus Layer,” CSUR, 2017.
[29] K. Yi, J. Lee, and H. Kim, “Post-Quantum Signatures for Blockchain Transactions,” IEEE Blockchain, 2020.
[30] Y. Liu et al., “Lightweight Post-Quantum Digital Signatures for Decentralized Applications,” Future Generation Computer Systems, 2022.