International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 1, 2026
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research

Quantum-Resistant Blockchain Using CRYSTALS-Dilithium for Secure Transactions

Y.Nagamalleswararao [1],K.Pavani[2],R.Bhargavi[3]

#1 Assistant Professor in the Department Of MCA, SRK Institute Of Technology,Vijayawada.

#2 Assistant Professor & Head of the Department of MCA, SRK Institute of Technology, Vijayawada.

#3 Student in the Department of MCA, SRK Institute of Technology, Vijayawada

Abstract: Cryptographic digital signatures are essential to blockchain systems' transaction integrity and authenticity. However, traditional encryption methods like RSA and Elliptic Curve Cryptography (ECC) are under threat from the quick development of quantum computing, leaving current blockchain infrastructures open to potential quantum assaults. In order to ensure transaction verification, this study suggests a quantum-resistant blockchain system that makes use of the CRYSTALS-Dilithium post-quantum digital signature technique. Interoperability between classical and post-quantum signatures is made possible by the use of a hybrid cryptographic technique. Additionally, before being stored on the blockchain, every transaction data is encrypted using the Advanced Encryption Standard (AES) to improve data confidentiality. A simulation environment that facilitates the creation and verification of multi-user transactions is used to construct and assess the suggested framework. While RSA has a shorter execution time, CRYSTALS-Dilithium gives far higher security assurances against quantum attackers, according to performance research utilizing latency measurements. The findings validate the viability and efficiency of combining encrypted data storage and quantum-resistant encryption for safe, future-proof blockchain transactions.

Index terms - *— Blockchain, Quantum Computing, Post-Quantum Cryptography, CRYSTALS-Dilithium, Digital Signatures, AES Encryption, Transaction Security.*

1. INTRODUCTION

Blockchain technology has emerged as a core paradigm for decentralized, transparent, and tamper-resistant transaction management across various domains including finance, healthcare, supply chain, and Internet of Things (IoT). Its security model relies heavily on cryptographic primitives such as digital signatures, hash functions, and consensus

mechanisms to ensure integrity, authenticity, and trust without centralized authorities.

Despite its robustness against classical computational attacks, blockchain faces significant risks due to the rapid evolution of quantum computing. Quantum algorithms such as Shor's algorithm can efficiently break RSA and ECC by solving integer factorization and discrete logarithm problems. This capability threatens transaction verification, private key security, and long-term data integrity in blockchain networks.

To address these challenges, there is an urgent need for quantum-resistant blockchain architectures that ensure cryptographic durability beyond the quantum era. This work focuses on integrating post-quantum digital signature mechanisms while maintaining compatibility with existing blockchain infrastructures, ensuring security, scalability, and long-term reliability.

2. LITERATURE SURVEY

a) Quantum secured blockchain framework for enhancing post quantum data security

Quantum computing, a development of classical computing, can solve problems competitive enough to breach blockchain systems' cryptographic primitives. Quantum algorithms (Shor's and Grover's) potentially undermine RSA, ECDSA, and SHA-256, raising concerns about blockchain-based applications in banking, healthcare, and supply chains. Current efforts focus on specific blockchain characteristics like cryptographic primitives or key exchange, without a complete plan to assure end-to-end security in the face of a quantum attack. Finally, Sybil attacks, centralization, and leader-selection bias can damage Proof-of-Work and Proof-of-Stake consensus processes. When the enemy gets a quantum computer, these concerns worsen. In this paper, we present QuantumShield-BC, a modular blockchain framework incorporating post-quantum cryptographic signatures, quantum key distribution (QKD), and a novel Quantum Byzantine Fault Tolerance (Q-BFT) consensus mechanism driven by quantum random number generation (QRNG) to address these challenges. QKD: Secure transaction signing, tamper-proof key exchange, and quantum-resilient validator node consensus are supported. QuantumShield-BC has short consensus time, great throughput, and flawless security against Shor's and Grover's algorithms in experiments. The proposed framework removes Sybil attacks, replay and MITM weaknesses, and achieves over 7,000 transactions per second with 100 validators, orders of magnitude faster than conventional blockchain systems. The system's resilience depends on each quantum portion, as shown by an ablation investigation. QuantumShield-BC is suitable for critical infrastructure and digital trust ecosystems that require performance and a future-proof foundation. It provides a post-quantum framework for high-assurance, general-purpose, scalable, and interoperable blockchain networks resistant to quantum-inspired attacks and retrieval.

b) Quantum-Resistant Privacy-Preserving IoT Authentication via Zero-Knowledge Proofs and Blockchain Integration:

Ensuring quantum resistance and privacy protection while keeping useful performance characteristics is a crucial problem for IoT device authentication. In order to provide secure IoT device management, this study introduces a unique privacy-preserving

authentication architecture that combines homomorphic encryption, blockchain technology, and zero-knowledge proofs (ZKPs). Through three major innovations—a lightweight post-quantum ZKP protocol, blockchain-based device verification with chameleon hash functions, and privacy-preserving homomorphic computation—our approach uniquely combines Security Module operations with blockchain-based verification to address the shortcomings of the current authentication methods. The system delivers state-of-the-art performance with 350 ms authentication times in our testing setting utilizing an Intel Core i7 platform with simulated IoT sensor networks, a 5.7% improvement over existing quantum-resistant methods. In a controlled test environment, the experimental findings show strong scalability, supporting 100 simulated devices at once with 98% GUI responsiveness while upholding privacy obligations. The Security Module achieves homomorphic encryption times of 180 ms and ZKP generation/verification speeds of 300/120 ms, respectively. We also demonstrate gas efficiency with device registration averaging 145,000 gas units and 150 ms network synchronization using a unique blockchain integration architecture. Without sacrificing scalability or efficiency, the framework creates workable quantum-resistant privacy-preserving authentication for Internet of Things contexts.

c) Examining the Security Role of Quantum-Resistant Smart Contracts in Protecting Sensitive Data in Blockchain Applications:

Since quantum computing is becoming a greater threat to conventional encryption, this study investigates the security of quantum-resistant smart contracts for data protection on blockchain networks. Making sure blockchain's security features are robust and reliable is essential as it becomes a fundamental component of vital digital networks. In order to improve quantum resilience, the study intends to assess the efficacy, efficiency, and viability of incorporating post-quantum cryptographic algorithms—specifically, CRYSTALS-Dilithium—into novel contract frameworks. A hybrid research design was used, combining performance evaluation, simulation-based testing, and theoretical analysis. Information was gathered from sources for cryptography measures, specialist blockchain platforms, and scientific research. Solidity, the Open Zeppelin libraries, and quantum-resistant cryptographic routines—which were incorporated through external frameworks—were used at every level of the creation and testing of smart contracts. Among the main metrics were information security principles including availability, confidentiality, and integrity. The system's effectiveness (in terms of gas cost, latency, and processing needs) and defense against quantum assaults were additional assessment factors. The findings showed that although while quantum-resistant smart contracts use more resources and have greater computing costs, they perform far

better in terms of security than conventional contracts, especially when it comes to quantum attacks.

d) Asynchronous Quantum-Resistant Blockchain for Secure Intelligence Sharing:

Organizations may develop a more thorough threat landscape knowledge and proactively detect possible hazards by compiling intelligence on new threats, attack methods, and vulnerabilities. However, businesses frequently reluctant to share threat intelligence because they are worried about information leaks, which lowers their motivation to work together. Additionally, the quality and reliability of shared data have been adversely affected by the lack of openness and confidence in intelligence sources. The authors want to use blockchain technology to solve these problems by ensuring corporate privacy and the dependability of intelligence sources through its decentralized and tamper-proof characteristics. A dual blockchain architecture is also used to improve operational effectiveness and lessen storage requirements. However, Shor's algorithm poses a danger to commonly used public key cryptography techniques, making existing cryptographic processes utilized in blockchain systems vulnerable to the emergence of large-scale quantum computing. Quantum-resistant cryptographic technologies, such as SPHINCS+ and CRYSTALS-KYBER, are integrated to enable quantum-safe migration in blockchain applications, guaranteeing system security and resilience in future quantum computing environments. This ensures long-term security and resilience in a quantum-enabled threat landscape.

e) An AI-Driven Framework for Integrated Security and Privacy in Internet of Things Using Quantum-Resistant Blockchain:

There are serious security and privacy issues brought about by the expanding use of the Internet of Things (IoT) in many industries. Comprehensive frameworks that successfully integrate cutting-edge technology to counter emerging threats are inadequate, despite the abundance of individual solutions. The Integrated Adaptive Security Framework for IoT (IASF-IoT), which combines blockchain technology, quantum-resistant encryption, and artificial intelligence into a single, IoT-specific solution, is presented in this study. The framework's main component is an adaptive AI-driven security orchestration system, which is enhanced with lightweight quantum-resistant protocols, blockchain-based identity management, and digital twins for threat prediction and proactive mitigation. The framework was assessed using a large-scale simulation with 1000 heterogeneous IoT devices and a theoretical performance model. The results demonstrated that IASF-IoT achieved detection accuracy ranging from 85% to 99%, with reaction times averaging about 2 s and simulated energy usage staying below 1.5 mAh per day. These results indicate that the framework has great potential for low-overhead, scalable security in IoT systems with limited resources.

3. METHODOLOGY

i) Proposed Work:

The proposed project designs a quantum-resistant blockchain architecture to protect transaction verification and data secrecy against quantum computing threats. The system replaces or supplements RSA and Elliptic Curve Cryptography

with the CRYSTALS-Dilithium post-quantum digital signature technique. A hybrid cryptographic paradigm allows blockchain networks to use classical or post-quantum signatures for interoperability and progressive migration without affecting blockchain infrastructures. This method improves transaction authentication, inhibits digital signature fraud, and maintains ledger integrity in quantum-vulnerable contexts. The proposed system uses lattice-based cryptographic primitives to withstand classical and quantum attackers while retaining decentralized trust and verification.

After quantum-resistant authentication, the proposed system encrypts all transaction data using the Advanced Encryption Standard before storing it on the blockchain to improve transaction privacy. This addon keeps transaction data private even if an attacker or unauthorized user has the smart contract address. The system design enables critical blockchain functions such transaction creation, signature generation, broadcasting, verification, block building, block signing, and consensus finalization. A simulation proves safe multi-user transactions, digital signature verification, and encrypted data storage are possible. Latency measurements show that the proposed project achieves scalable, secure, and future-proof blockchain transaction management for post-quantum environments by balancing computational efficiency and security.

ii) System Architecture:

The proposed quantum-resistant blockchain framework supports safe, decentralized, post-quantum transaction processing with a layered modular architecture. Registration, authentication, transaction generation, and verification are done using a web-based interface for registered users. The application layer collects sender, receiver, transaction amount, and timestamps for transaction generation. A hybrid cryptographic interface supports traditional RSA/ECC signatures and the CRYSTALS-Dilithium post-quantum signature technique that generates digital signatures. To maintain secrecy, transaction data is encrypted using AES before transmission. The blockchain stores and validates this encrypted and signed transaction.

The blockchain layer handles transaction broadcasting, signature verification, block construction, hashing, and consensus finalization. Before accepting transactions into a block, each blockchain node checks CRYSTALS-Dilithium signatures using public keys to assure authenticity and integrity. Hash functions connect blocks for immutability and tamper resistance. Smart contracts on the blockchain store user data and transactions securely and transparently. A performance analysis module records execution time and creates latency graphs comparing RSA and CRYSTALS-Dilithium algorithms. This layered and modular design assures scalability, interoperability, and long-term durability, allowing secure blockchain operations even against quantum-capable attackers.

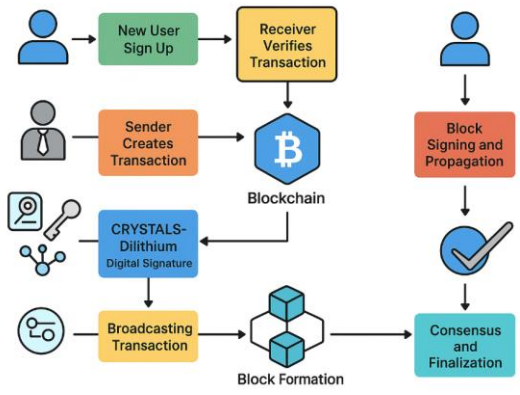


Fig1 proposed architecture

iii) Modules:

a. New User Sign-Up:

By supplying necessary identification information, this module allows new users to register within the blockchain system. User data is safely saved on the blockchain after successful registration, guaranteeing identity management that is tamper-resistant, genuine, and traceable. The decentralized network's participants' confidence is bolstered by the unchangeable storage of user information, which facilitates trustworthy transaction verification.

b. Log in as a user:

Before granting registered users access to system features, the login module verifies their identity. The module makes sure that only authorized users may start transactions or validate blockchain data by verifying user credentials. The secrecy and integrity of blockchain processes are preserved by this procedure, which also stops unwanted access.

c. Transaction Creation by Sender:

By providing the recipient, transaction amount, and date, this module enables verified users to create blockchain transactions. To provide safe authentication, every transaction is digitally signed using the CRYSTALS-Dilithium post-quantum signature technique. Furthermore, before being broadcast and recorded on the blockchain, the whole transaction data is encrypted using AES to prevent unauthorized disclosure of sensitive information.

d. Verify the transaction with the recipient:

The CRYSTALS-Dilithium signature verification procedure is used by the receiver verification module to retrieve stored blockchain transactions and confirm their legitimacy. AES-encrypted data guarantees the confidentiality of important transaction details, while digital signatures verify the integrity and origin of transactions. Multiple users can safely validate transactions with this module without disclosing unencrypted information.

e. Graph of Latency:

This module measures and displays transaction execution delay in order to assess system performance. For different transaction volumes, a latency graph comparing the suggested CRYSTALS-Dilithium method with traditional RSA is produced. The analysis supports the performance evaluation of the suggested framework by highlighting the trade-off between improved post-quantum security and computing efficiency.

2. TECHNIQUES

a) RSA Cryptographic: RSA supports comparative latency evaluation by offering a classical public-key benchmark against which quantum-resistant alternatives can be assessed. Its workflow comprises genesis of key-pairs and modular exponentiation to sign or encrypt the selected data that could be used to count the execution time with various loads of transactions. The algorithm helps to identify the trends of the scalability of the common overheads of operation and performance constraints of the traditional cryptographic schemes of a decentralized configuration. Though computationally efficient, RSA is susceptible to quantum attacks and its addition is used to set a baseline against which security-performance trade-offs in cryptographic changes to post-quantum protocols can be thought of.

b) Blockchain Hashing: In blockchain hash hash algorithms, each block is converted into a fixed size hash of the stored data and uses this hash as a unique identifier of the stored data. During the creation of blocks, hashing mechanism is employed in such a way that the records of the next block are connected with the previous digests forming an irreversible chain that will not enable any party outside to change the historical records. This is a mechanism that strengthens the data integrity, provides a transparent auditability and facilitates effective verification of the sequences of transactions without revealing sensitive information. The linking structure that is based on hash helps generate trust, consistency of time sequence, and resistance against tampering and corruption of the data among

distributed nodes that are engaged in consensus-based functions.

c) Blockchain Consensus Mechanism: The consensus mechanism coordinates the distributed nodes to collectively verify transactions along with the addition of new block to the one that already exists and make them all share the same ledger state. Its operations include the publication of the transactions, verification by the independent nodes, conflict resolution and ultimate sealing of the blocks which ensures that it only approves legitimate entries. The mechanism provides greater tolerance to faults and system reliability by removing the chances of two or more transactions being executed with the same object and causing malicious interference of any nature. Coordinated decision-making supports secure propagation of authenticated data, enhances robustness under network variation, and provides a stable computational foundation for executing verified operations in decentralized environments.

4. EXPERIMENTAL RESULTS

A Python simulation environment and a blockchain-enabled smart contract platform were used to construct and assess the suggested quantum-resistant blockchain framework. Multiple users can utilize the system to carry out safe tasks such transaction generation, verification, authentication, and registration. Before being deposited on the blockchain, transactions were encrypted using AES and digitally signed using the CRYSTALS-Dilithium method. All produced transactions were successfully broadcast, validated, and immutably stored across blockchain nodes, according to experimental findings. Receiver-side verification showed that digital signatures were correctly validated while data confidentiality was maintained since unauthorized users could not access encrypted transaction fields. Block numbers, transaction hashes, and verification status were shown in the simulation logs, which verified proper block generation and tamper-resistant storage.

In order to compare the suggested CRYSTALS-Dilithium post-quantum signatures with traditional RSA-based signatures, performance assessment concentrated on transaction delay analysis. A comparison graph was used to display the latency metrics as the number of transactions increased. The findings show that RSA's computational simplicity results in shorter execution times, but it is not resistant to quantum assaults. CRYSTALS-Dilithium, on the other hand, offers far better security assurances appropriate for post-quantum systems, albeit at the expense of increased latency. The experimental findings show that the suggested system achieves acceptable computing efficiency while guaranteeing strong quantum-resistant transaction verification and encrypted data protection in blockchain applications, highlighting a clear trade-off between speed and security.

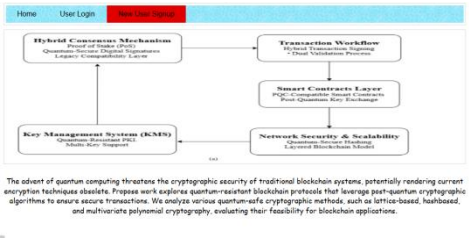


Figure 2: Application Home Page

This image displays the home page of the blockchain application that has been accessed via a browser. Mostly, it offers the possibility to navigate through New User Sign-Up, User Login, Transaction Creation, Verification, and Performance Analysis options, and allows the user to interact with the blockchain system.

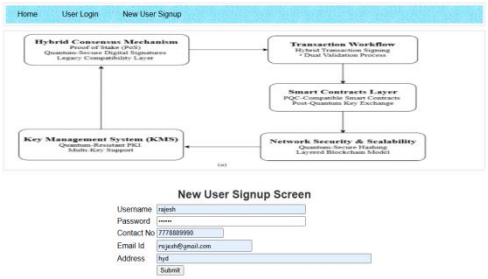


Figure 3: New User Sign-Up Interface

This figure illustrates the user registration module in which new users are required to fill their personal and login details. When submitted, the user data is safely stored in the blockchain, and this guarantees identity management that is tamper-resistant.

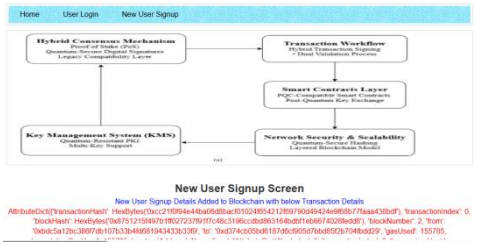


Figure 4: User Registration Stored in Blockchain

This number depicts a successful user registration data storage on the blockchain. The presented log data consists of block number, transaction number and hash values, which prove the immutable storage and the effective creation of blockchain entries.

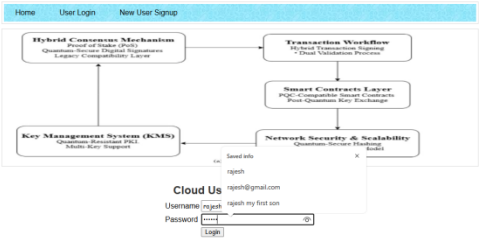


Figure 5: User Login Interface

This figure presents the authentication component in which the registered users use valid credentials to log in. A successful login establishes a valid access to system capabilities and stops unlicensed blockchain communication.

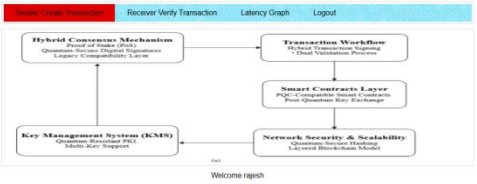


Figure 6: Create Transaction Interface

This value illustrates the transaction creating module in which a sender picks a receiver, key in the amount of the transaction and a blockchain transaction is initiated. The interface gathers all the necessary transaction details to make the transactions secure.

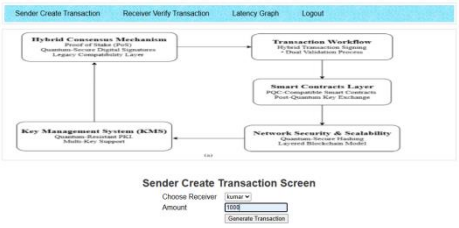


Figure 7: Create Transaction Interface

This value illustrates the transaction creating module in which a sender picks a receiver, key in the amount of the transaction and a blockchain transaction is initiated. The interface gathers all the necessary transaction details to make the transactions secure.

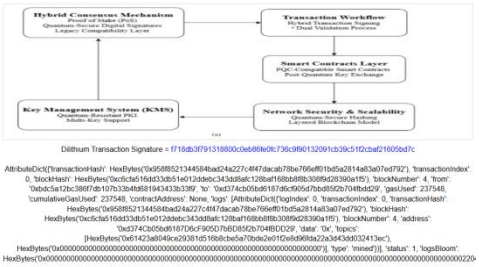


Figure 8: Digital Signature Generation and Blockchain Storage

This diagram depicts the creation of a digital signature with the use of CRYSTALS-Dilithium algorithm. The data of the signed transaction is encrypted with AES and stored on the blockchain, and the logs of the blockchain block confirm the successful creation of a block.

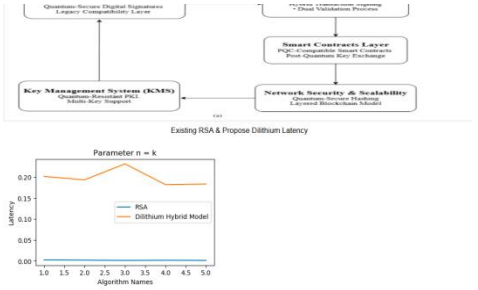


Figure 9: Latency Comparison Graph

This value shows the latency comparison of classical RSA and the suggested CRYSTALS-Dilithium algorithm. The x-axis is the number of transactions, whereas the y-axis is latency, and it is evident that RSA is quicker and less secure but CRYSTALS-Dilithium is more secure as it is quantum-resistant.

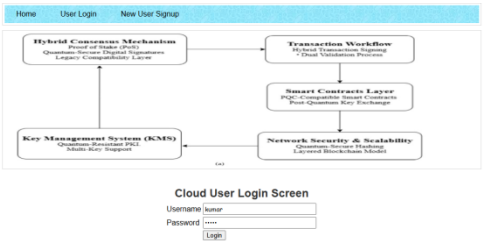


Figure 10: Receiver Login Interface

This figure displays the login screen for the receiver user. It confirms that multiple users can independently access the system and verify transactions stored on the blockchain.

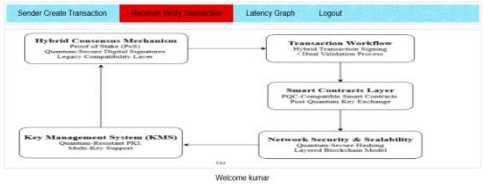
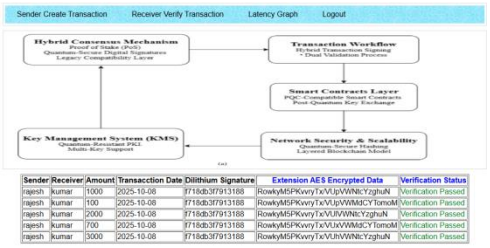


Figure 11: Receiver Transaction Verification Interface

This figure presents the transaction verification module where receivers view transaction records retrieved from the blockchain. Digital signatures are verified using CRYSTALS-Dilithium, ensuring transaction authenticity and integrity.



Sender	Receiver	Amount	Transaction Date	Dilithium Signature	Extension AES Encrypted Data	Verification Status
rajesh	kumar	1000	2025-10-08	f718db3f7913188	RowkyM5PKvvyTxVUpVWNtCYzghuN	Verification Passed
rajesh	kumar	100	2025-10-08	f718db3f7913188	RowkyM5PKvvyTxVUpVWMdCYTomoM	Verification Passed
rajesh	kumar	2000	2025-10-08	f718db3f7913188	RowkyM5PKvvyTxVUtVWNtCYzghuN	Verification Passed
rajesh	kumar	700	2025-10-08	f718db3f7913188	RowkyM5PKvvyTxVUxVWMdCYTomoM	Verification Passed
rajesh	kumar	3000	2025-10-08	f718db3f7913188	RowkyM5PKvvyTxVUhVWNtCYzghuN	Verification Passed

Figure 13: Successful Signature Verification Result

This figure confirms that all retrieved transactions have been successfully verified. The verification status indicates valid digital signatures, proving correct implementation of post-quantum signature verification and secure transaction validation.

5. CONCLUSION

The CRYSTALS-Dilithium post-quantum digital signature technology and encrypted data storage were used to create a quantum-resistant blockchain system that improves transaction security. Because a hybrid cryptography technique is used, the system is safe against quantum computing risks and compatible with traditional RSA and ECC procedures. Immutable blockchain storage, safe multi-user transaction generation, and verification were demonstrated using simulations. Experimental results show that while CRYSTALS-Dilithium takes longer to compute than RSA, it provides better security guarantees for post-quantum scenarios. All transaction data was encrypted using AES to maintain confidentiality and stop data theft. The suggested architecture is a viable future-proof blockchain transaction management solution in quantum-vulnerable digital ecosystems because it blends security, scalability, and usefulness.

6. FUTURE SCOPE

Future work can focus on deploying the proposed quantum-resistant blockchain framework in large-scale, real-world decentralized environments to evaluate performance, scalability, and security under dynamic network conditions. Integration of advanced post-quantum key management techniques and lightweight cryptographic optimizations can further improve efficiency, especially for resource-constrained platforms such as IoT systems. Enhancing interoperability across multiple blockchain platforms and enabling seamless migration from classical to post-quantum cryptography will support wider adoption. Additionally, incorporating privacy-preserving mechanisms such as zero-knowledge proofs and adaptive consensus protocols can strengthen data protection and system resilience. Further research can also explore reducing computational overhead and improving transaction throughput while maintaining strong quantum-resistant security guarantees.

REFERENCES

[1] A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, ‘‘Quantum computers put blockchain security at risk,’’ Nature, vol. 563, no. 7732, pp. 465–467, Nov. 2018.

[2] D. J. Bernstein and T. Lange, ‘‘Post-quantum cryptography-dealing with the future,’’ Nature, vol. 549, no. 7671, pp. 188–194, Sep. 2023.

[3] G. Alagic et al., ‘‘Status report on the third round of the NIST post-quantum cryptography standardization process,’’ NIST, Tech. Rep., 2024.

[4] R. Román, R. Arjona, P. López-González, and I. Baturone, ‘‘A quantumresistant face template protection scheme using kyber and saber public key encryption algorithms,’’ in Proc. Int. Conf.

Biometrics Special Interest Group (BIOSIG), Sep. 2022, pp. 1–5.

[5] M. Mosca and C. Paquin, ‘‘Quantum-safe cryptography integration in blockchain networks,’’ Cryptol. ePrint Arch., Report 2024/123, 2024.

[6] T. Pabla and A. Sultana, ‘‘Modular blockchain architecture: Securing data with quantum-safe encryption,’’ in Proc. Int. Conf. Quantum Commun., Netw., Comput. (QCNC), Jul. 2024, pp. 198–203.

[7] D. J. Bernstein, ‘‘SPHINCS+: Submission to NIST post-quantum cryptography standardization,’’ Tech. Rep., 2024.

[8] R. J. McEliece, ‘‘A public-key cryptosystem based on algebraic coding theory,’’ DSN Prog. Rep., vol. 44, pp. 114–116, Jan. 1978.

Author Profiles



Mr. Y. Nagamalleswararao completed his Master of Technology (M.Tech) from JNTUK, M.Sc (IS) from ANU, and BCA from ANU. He has expertise in System Administration, Network Administration, and Oracle Administration. He is also a Web Developer and Python Developer. Currently, he is working as an Assistant Professor in the Department of MCA at SRK Institute of Technology, Enikepadu, NTR District. His areas of interest include Artificial Intelligence and Machine Learning.



Ms. K. Pavani is working as an Assistant Professor and Head of the Department of MCA at SRK Institute of Technology, Vijayawada. She completed her M.Tech and MCA in Computer Science. She has 10 years of teaching experience at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. Her areas of interest include Machine Learning with Python and DBMS.



Ms.R.Bhargavi is an MCA Student in the Department of Computer Application at SRK Institute Of Technology, Enikepadu, Vijayawada, NTR District. She has Completed Degree in B.Sc.(computer science) from AG&SG Siddharth college of arts and science vijayawada. Her area of interest are Machine Learning with Python.