

Quantum-Resistant Blockchain Protocols For Secure Transactions

Kollikondla Praneeth Kumar^{1*}, Dr. V. Valli Mayil², Sushmitha M³, Tummapudi Sunil⁴

¹Student, Department of Computer Science and Engineering, KL UNIVERSITY, Andhra Pradesh, India.

²Professor, Department of Computer Science and Engineering, KL UNIVERSITY, Andhra Pradesh, India.

³Assistant Professor, Department of Computer Science and Engineering, Sri Krishna Institute of Technology.

⁴Assistant Professor, Department of AIML, SRK Institute of Technology, Enikepadu, Vijayawada.

*correspondence mail: praneeth.klu@gmail.com

Abstract

Background: Digital signatures are crucial for ensuring the authentication of deals in a blockchain system. The introduction of quantum computing, however, can be a real danger to these types of systems, as it allows for hackers to break the widely used cryptographic systems, such as RSA, ECC and AES. To overcome this shortcoming, a quantum-resistant digital signature verification mechanism using the CRYSTALS-Dilithium algorithm is suggested for securing transactions in the post-quantum era. The method is based on a signature architecture mixture of classical and quantum -safe methods, providing backward compatibility and enhanced security. This process consists of transaction creation, digital signature, transaction broadcasting, transaction validation, and block formation and a consensus. User registration and transaction processing is carried out by smart contracts in a tamper-proof Blockchain ecosystem. In addition, the data of transactions are protected from unauthorized transactions and ensured privacy is maintained by AES. Performance investigation shows that the hybrid CRYSTALS-Dilithium algorithm has somewhat higher latency than RSA and ECC, but greatly enhances resilience to quantum attacks. In conclusion, the combination of quantum-safe cryptography and Blockchain promises to create a robust and sustainable platform for future digital transactions, providing long-term security, scalability, and interoperability for decentralized systems.

Keywords: Blockchain security, decentralized networks, post-quantum cryptography, quantum computing, quantum-resistant protocols, secure transactions.”

1. Introduction

The blockchain technology has emerged as an innovative approach to secure digital transactions in recent years, providing trusted, transparent and immutable security across decentralized networks [1]. It has been used widely in the IoT, finance, supply chain management, and many other applications due to its reliance on cryptographic primitives [2]. At the same time, the fast development of quantum computing is changing the technical environment by providing amazing processing power [3]. These developments have led to a greater push for greater global research on studying and bolstering existing digital security structures [4]. With the growth in volume and complexity of blockchain systems, the issue of computational threats and how these can be thwarted over time has been actively pursued and investigated [5].

While the current blockchain architectures are robust, the security of the designs is now under threat as a result of the advent of quantum computing, a powerful threat to classical cryptographic systems [6]. Important concerns regarding the viability of existing blockchain protocols are related to the quantum algorithms that can break the widely used public-key schemes [7]. There are several studies that have investigated the theoretical implications of quantum attacks, but it is still not known how to systematically make blockchain infrastructures more compatible with future cryptographic environments [8]. Up until now, no full systems have emerged from study that will ensure blockchain networks are safe and effective in a post-quantum world. This suggests further investigations should be carried out.

The research objective is to develop more secure approaches for blockchain systems in a quantum era, which are not vulnerable to quantum computers. The study focuses on issues of compatibility, speed and changes in the architecture that facilitate safe collaboration between computers when they are under threat. This paper is a continuous attempt at enhancing security research on the blockchain. It does so by studying existing vulnerabilities and potential future research into enhancing blockchain cryptography. To provide a clear understanding of the

potential future evolution of blockchain communities, in a manner that supports privacy, trust and honesty while technology evolves rapidly.

This contributes to the development of next-generation blockchain infrastructures that will be capable of resisting quantum attacks, thereby assuring the stability of decentralized systems [10]. With industries relying more on blockchain technology for mission-critical applications, laying the foundations for quantum-resilient security is essential to protect digital assets and ensure operational integrity. The findings of such research will be beneficial for policy makers, system architects and security practitioners in the development of resilient, sustainable, scalable and future-proof blockchain solutions in the face of rapid advances in the computing front.

2. Literature review

The increasing interest in post-quantum security has resulted in a large body of research studying quantum-resistant solutions for blockchain applications. In a world where AI is increasingly becoming a major player, Adelusi et al. [11] explored quantum-resistant cryptographic approaches to ensure the security of financial transactions and the need to safeguard sensitive corporate data. Their work stresses the need for post-quantum systems, but it is mostly conceptual and gives no information about how to incorporate them into decentralized infrastructures. Liu et al. [12] have given a Quantum resistant Sharding Blockchain Architecture to achieve safe data transfer. The study demonstrated improved scalability and resilience, but not yet a good deployment of the sharding techniques.

One of the first works that demonstrated the application of post-quantum cryptographic primitives for DLs is the blockchain proposed by Zhang et al. [13] that introduces quantum-resistant digital signatures. Although the implementation was encouraging, the study focused on the signature schemes narrowly and did not discuss system-level performance implications. Unogwu et al. [14] conducted an extensive study of quantum-resistant blockchain technology, giving a background of the impending threats and possible solutions. They make significant theoretical advances, but there is no empirical evaluation and it's unclear how it works in the real world. Sinai and In [15] performed a performance study of quantum resistant blockchain techniques and compared with traditional signatures such as Secp256k1 and Schnorr. The outcomes revealed compromises in performance without any architectural changes that would decrease the latency and computational cost were explained in the work.

More work is required for domain specific applications. B. Balasubramaniam and . S. A quantum-resistant blockchain paradigm for smart city transaction was proposed by [16] with its potential of improving the security of inter-connected urban systems. The design was not meeting the need for interoperability with existing infrastructures, however. In an attempt to prevent phishing attacks on blockchain wallets, Sahu et al. [17] studied post-quantum cryptography. They emphasized the need for user-level security enhancement. The majority of the work was centred around threats on the application layer, and not on threats to the underlying blockchain, which is applicable. To improve transaction integrity in decentralized financial ecosystems, Muda et al. [18] introduced a new blockchain protocol. However, the study focused mostly on integrity mechanisms, rather than quantum-specific hazards.

The growing imperative to be quantum ready continues to be demonstrated in more studies. New studies keep pointing to a rising need for quantum readiness. Zahoor and De Roest [19] emphasized the need to shift over to quantum resistant blockchain systems and pointed out the significant challenges to obtain enduring security. However, they were at a high level of work, and did not present specific architectural models. Peelam and Chamola [20] explored the quantum improved blockchain architectures for consumer IoT networks and demonstrated potential enhancements to consumer IoT networks' defence against novel threats. This research, however, was conducted in IoT contexts only and could not be applied to other blockchain contexts.

Overall, it highlights the importance of quantum resilience, but also identifies ongoing gaps, including: a lack of holistic system-level evaluations, limited attention to scalability, and a lack of integrated approaches to practical implementation. To tackle these challenges, the current study proposes a comprehensive security-oriented blockchain framework that ensures ongoing security when facing quantum-enabled threats without sacrificing operational efficiency in different decentralized environments.

3. Materials and methods

The proposed solution provides a quantum safe Blockchain foundation for secure and confidential digital transactions in quantum era. The method is hybrid, where classic RSA/ECC is used in conjunction with the CRYSTALS-Dilithium signature scheme to ensure robustness without sacrificing backward compatibility. Transaction data is created, signed, broadcasted, validated and added to block via a streamlined process, user registration is automatic and transaction data is permanently recorded by smart contracts on the Ethereum Blockchain. All transaction data is further confidentialized by being encrypted with AES when it is leaked, even contract details, no sensitive data is leaked. Reliable authentication, immutability and privacy protection of the system are demonstrated by creating and testing secure transactions using dummy data. The proposed plan to combine quantum-safe signatures, symmetric encryption, and decentralized contract execution is designed to create a robust, scalable, and future-proof Blockchain ecosystem that will be able to address the new threats posed by quantum computers.

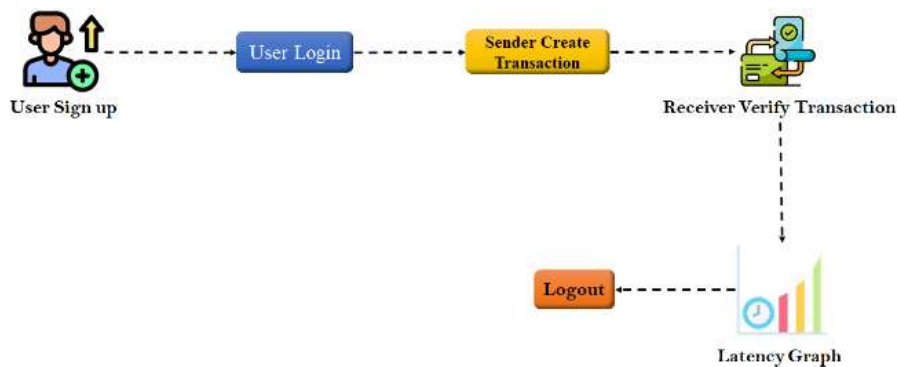


Fig.1 Proposed Architecture

a) Modules:

New User Sign Up: New users can register by providing the essential data like name, email, secure credentials etc. in the module. All registration information is stored on the Blockchain to guarantee that the registration information is kept immutable and tamper-proof. The module facilitates secure identity management in a decentralized environment, sets up user accounts, and grants users access to system functions like transaction creation, data verification, and interaction with smart contracts.

User Login: This module authenticates the user credentials from the records kept in Blockchain for secure and secured access. It is used to prevent unwanted entrance and keep the privacy of the user intact by using the immutable data of the Blockchain to verify. Once users log in, they can create transactions, confirm the data that has been uploaded, interact with smart contracts, and see all the activities in the system. The module guarantees the adherence to the principles of responsibility, integrity and limited access when interacting the user with the platform.

Sender Create Transaction: This module enables to create new transactions by entering the receiver information, amount of transaction and the timestamp. The transactions are signed with the CRYSTALS-Dilithium cryptographic method, ensuring authenticity and resistance to quantum attacks. Once signed, the transaction is then broadcasted to all Blockchain nodes for its verification, storage and spread into blocks. This module will provide the ability to create deals securely and effortlessly join the decentralized ledger.

Receiver Verify Transaction: This module allows Receivers to view, see and confirm transactions that have been pulled from the Blockchain. It verifies that the transaction is legitimate and has not been altered by comparing the digital signature to the key that matches it, and that it has been safely recorded. The module ensures integrity and authenticity, thus allowing the user to be confident that transactions received are trustworthy before they accept them and take any additional action. It helps in fostering transparency and trustworthiness in the Blockchain verification procedure.

Latency Graph: This module provides visual performance knowledge of transaction delay information. The execution time of standard algorithms like RSA and ECC is compared with hybrid CRYSTALS-Dilithium method, which demonstrates the difference in efficiency of execution. Users can get insights into patterns, test system performance and understand the performance vs security compromises of quantum-resistant systems. It enables performance monitoring and decision making for cryptography setup.

Logout: This module will end the Users session safely and prevent unauthorized access. It clears temporary session objects, finishes user activities and ensures privacy and security after the use of the system. It guards the system's integrity by closing authenticated sessions appropriately and by limiting the possibilities for the abuse of the current login sessions. The module has a safe exit protocol and also ensures the accountability of all transaction and operations that take place during the session.

b) Methods/Technologies:

CRYSTALS-Dilithium Algorithm: CRYSTALS-Dilithium is a post-quantum digital signing method that can't be broken into using quantum computers. It introduces safe Public-Private Key pairs into the system and validates the transactions on the Blockchain nodes' signatures. It offers resistance to quantum attacks, preventing counterfeiting and instilling trust in decentralized environments. Dilithium is used in the answer to make sure that Blockchain transactions are secure and can't be changed, even from advanced quantum computing attacks.

AES (Advanced Encryption Standard): AES is symmetric encryption that can be used to secure private transaction data prior to its placement on the Blockchain. This means that information cannot be seen by anyone even if someone gains access to the ledger. AES is effective, fast and is not susceptible to cryptanalysis. With the addition of digital signatures, it safeguards privacy and integrity, creating a more secure and less susceptible form of Blockchain storage from hackers and other external threats.

ECC (Elliptic Curve Cryptography): ECC is a cryptographic technique based on asymmetric cryptography. It offers high security and lesser key size and computational complexity. It is used within the system in the hybrid signature model, in order to be compatible with the existing Blockchain infrastructures. ECC is not quantum resistant per se, but can be utilized by classical nodes for secure signing, key generation and verification. Its inclusion enables seamless compatibility between conventional and post-quantum cryptography so that users may gradually move towards quantum-safe Blockchain security.

RSA Algorithm: RSA is an old asymmetric encryption method, applied for signing and safe operations with keys. In this system, they want to integrate hybrid signature model to make the existing Blockchain systems backward and inter-friendly compatible. In a normal day-to-day situation, RSA can be used to ensure authentication and transaction integrity, even if it is vulnerable to quantum attacks. It enables users who are fluent with legacy systems to operate safely and smoothly as they migrate towards quantum resistant digital signature schemes.

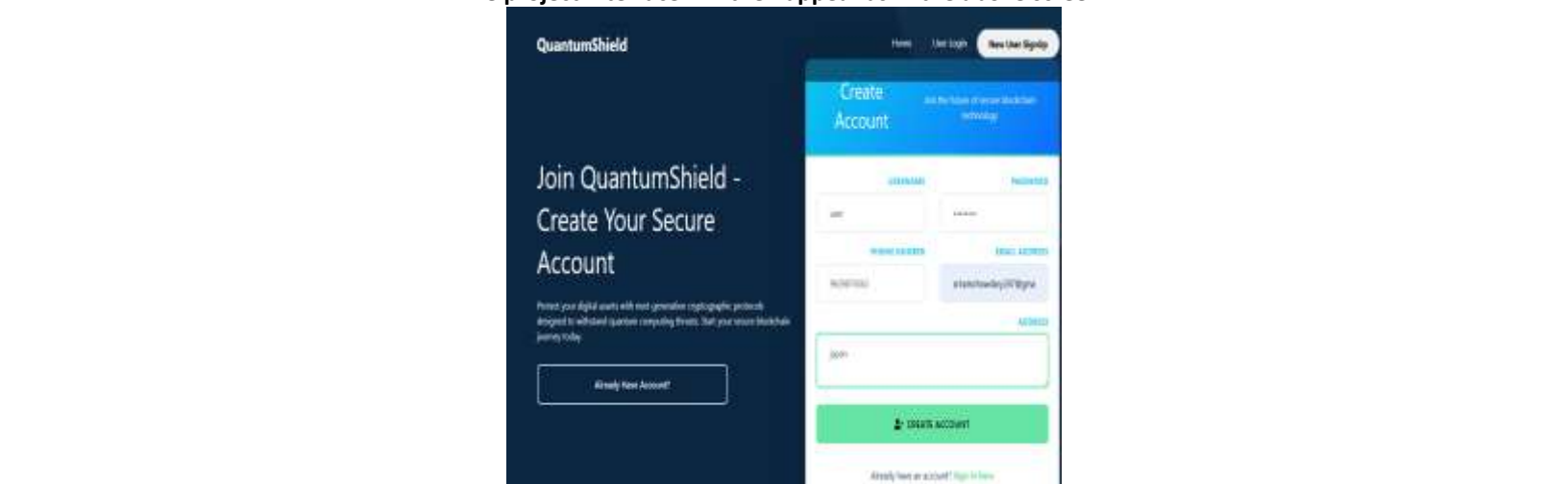
Blockchain Consensus Mechanisms (PoS/PBFT): Consensus mechanisms such as Proof-of-Stake and PBFT ensure a reliable consensus within the Blockchain network, about the authenticity of transactions and the creation of blocks. They enable the finalization of the blocks securely even if the conditions are adversarial and they preserve integrity and prevent double spending. These system processes coordinate the checking of transactions, the creation of blocks and the blocks' dissemination between nodes. They're used to ensure decentralized trust, regular updates of the state and tamper-proof ledger management, which is done without an intermediary.

Smart Contracts: Smart contracts are self-executing programs sitting inside the Blockchain that are able to automate the process of user registration, transaction processing and data verification. They apply pre-determined rules on all activities. This eliminates the need for manual involvement and prevents illegal changes. In the system, smart contracts are in charge of encrypted storage of transactions and hybrid signature processing, with secure interaction with users. The combination of the two promotes efficiency, transparency and dependability with retaining the decentralized control and adherence to the security protocol.

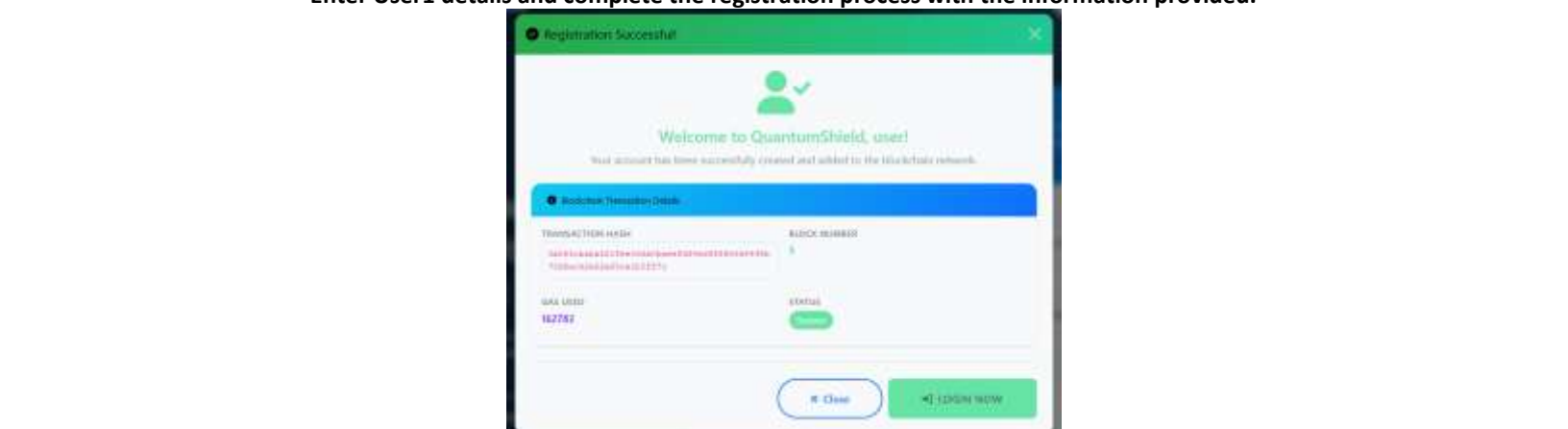
4. Experimental results



The project interface will then appear as in the above screen.



Enter User1 details and complete the registration process with the information provided.



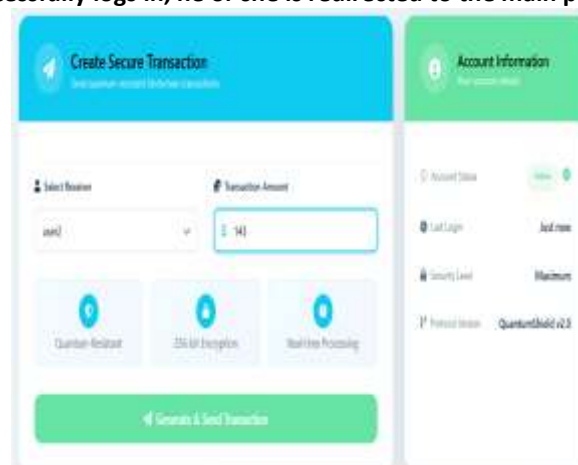
After the registration, the information of User1 is recorded on the blockchain, such as block number, transaction hash and gas consumption.



Give the User1 login information (User1's username and password) to log in to the account.



If User1 successfully logs in, he or she is redirected to the main page, as above.



Select the user2 and input the amount of the transaction to ensure a safe one, basic quantum features.

The image shows a two-part view of the QuantumShield website. On the left is a dark blue hero section with the QuantumShield logo at the top left. Navigation links 'Home', 'User Login', and 'New User SignUp' are at the top right. The main heading reads 'Join QuantumShield - Create Your Secure Account'. Below this is a paragraph: 'Protect your digital assets with next-generation cryptographic protocols designed to withstand quantum computing threats. Start your secure blockchain journey today.' At the bottom of this section is a button that says 'Already Have Account?'. On the right is a light blue 'Create Account' form. The form has a title 'Create Account' and a subtitle 'Join the future of secure blockchain technology'. It contains four input fields: 'USERNAME' (with placeholder 'user2'), 'PASSWORD' (with placeholder 'password'), 'PHONE NUMBER' (with placeholder '9876543210'), and 'EMAIL ADDRESS' (with placeholder 'stranchoudary247@gmail.com'). Below these is a 'SELECT ROLE' dropdown menu. At the bottom of the form is a 'confirm' input field. A green button with a person icon and the text 'CREATE ACCOUNT' is positioned below the form. At the very bottom of the right section, it says 'Already have an account? Sign in here'.

The image displays two versions of a login interface for an application named "QuantumShield".

Left Panel (Dark Theme):

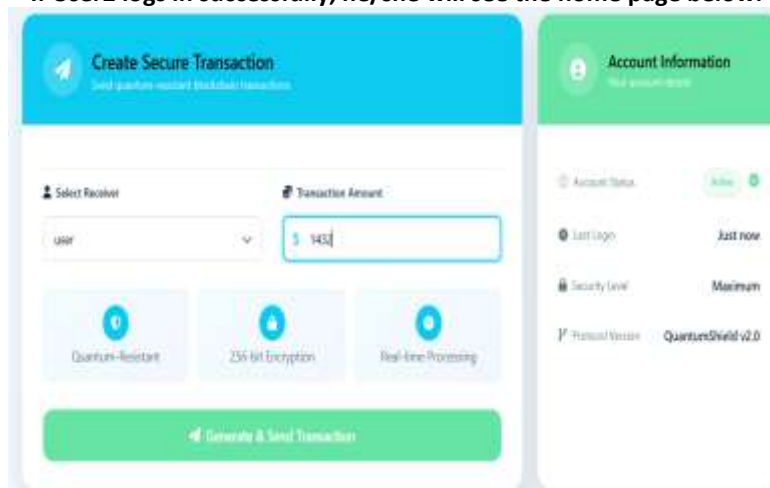
- Header:** "QuantumShield" logo on the left, and navigation links "Home" and "User Login" on the right, with a "New User Sign Up" button.
- Main Content:**
 - Greeting: "Welcome Back to QuantumShield"
 - Description: "Access your secure blockchain account and continue protecting your digital assets with quantum resistant protocols. Your security is our priority."
 - Buttons: "Need an Account?"

Right Panel (Light Theme):

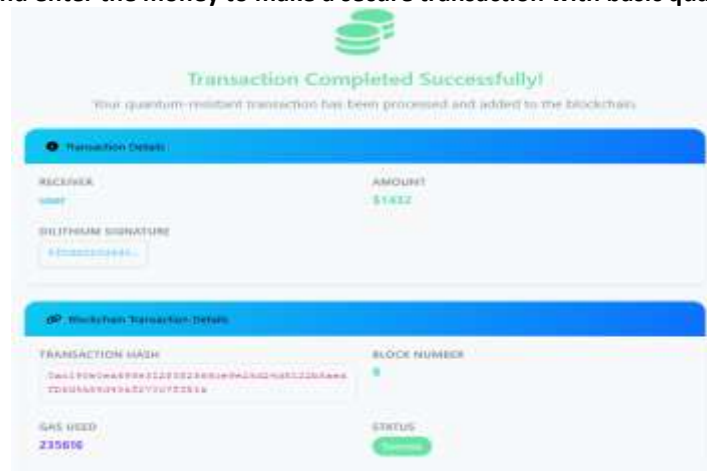
- Header:** "Sign In" title and "Access your secure account" subtitle.
- Form Fields:**
 - Email field with placeholder "EMAIL" and label "EMAIL ADDRESS".
 - Password field with placeholder "*****" and label "PASSWORD".
- Options:**
 - Remember me checkbox with label "Remember me".
 - Primary button: "SIGN IN".
 - Link: "Don't have an account? Create one here".



If User2 logs in successfully, he/she will see the home page below.



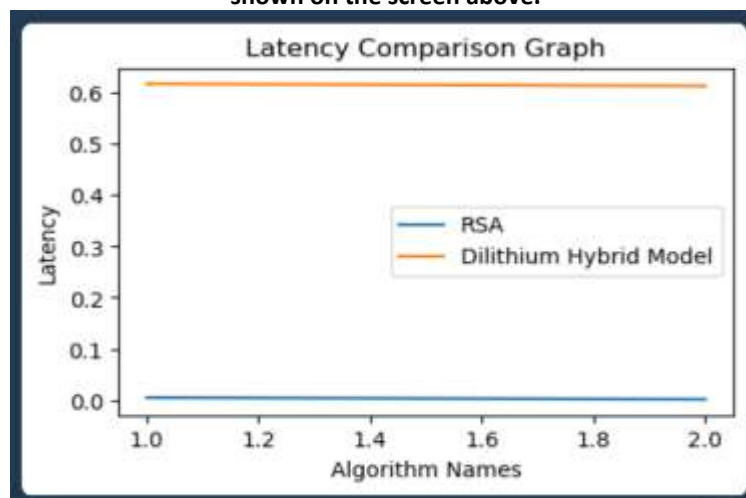
Choose the user1 and enter the money to make a secure transaction with basic quantum characteristics.



A list of the entire transaction history is shown along with the receiver's information, the amount, the hash of the block it is contained in, the block number, the gas consumed and status.



If the transaction verification is successful, then the AES encryption with the verification signature data will be shown on the screen above.



The following screen shows the graphs of the latency comparison of the implemented algorithms.

5. Conclusion

The adoption of quantum-resistant cryptographic techniques in Blockchain offers a solid and secure foundation for future digital ecosystems. The system uses the CRYSTALS-Dilithium algorithm for digital signatures to overcome the vulnerabilities of the present-day cryptographic systems, including RSA, ECC, AES, etc., in the light of quantum computing. The hybrid method also has the potential for seamless interoperability between classical and quantum-safe cryptographic algorithms and compatibility with older systems, while reducing the impact of new quantum cryptographic attacks. It is designed to create, sign, validate, and agree on secure transactions, making sure that there is end-to-end trust and integrity for decentralized networks. Smart contracts provide more automation and transparency and AES encryption ensures that only the authorized user has access to the data, leaving nobody else with access. Proposed paradigm has a somewhat higher latency than traditional systems. The downside, however, is a much better security and robustness. To sum up, the advent of post-quantum cryptography adds a new element to Blockchain's defense, ensuring the reliability, scalability, and sustainability of digital transactions in an increasingly quantum-powered world.

The quantum resistant cryptography system is to be extended to other Blockchain platforms in the future scope of the system to achieve global post-quantum security. The CRYSTALS-Dilithium method could be further improved by reducing the delay and computational cost, and improving efficiency while not compromising security, through

further study. A hybrid approach combining consensus methods and quantum-safe verification can be adopted for increased network resilience. Furthermore, security of quantum key distribution and other lattice cryptography systems could be significantly stronger. The platform will be further challenged by real-time financial, health and IoT applications to ensure its scalability, interoperability and readiness for future quantum-driven applications.

References

1. Dhayal, D., Varshney, P. K., & Wadhwani, G. K. (2025, July). Quantum-Resistant Blockchain Authentication Protocol: Securing Decentralized Systems Against Post-Quantum Attacks. In 2025 2nd International Conference On Multidisciplinary Research and Innovations in Engineering (MRIE) (pp. 786-790). IEEE.
2. Alutaibi, A. I. (2025). Quantum-Resilient Blockchain for Secure Digital Identity Verification in DeFi. *Computers, Materials & Continua*, 85(1).
3. Kapoor, A. (2025). Quantum-Resistant Cryptographic Frameworks for Securing Blockchain-Based Financial Transactions. Available at SSRN 5363211.
4. Reddy, N. R., Suryadevara, S., Reddy, K. G. R., Umamaheswari, R., Guttula, R., & Kotoju, R. (2025). Quantum secured blockchain framework for enhancing post quantum data security. *Scientific Reports*, 15(1), 31048.
5. Ashogbo, A. D., & Mosud, O. (2025). Examining the Security Role of Quantum-Resistant Smart Contracts in Protecting Sensitive Data in Blockchain Applications. *J Electrical Electron Eng*, 4(5), 01-08.
6. Wu, F., Zhou, B., Song, J., & Xie, L. (2025). Quantum-resistant blockchain and performance analysis. *The Journal of Supercomputing*, 81(3), 498.
7. Thanalakshmi, P., Rishikesh, A., Marion Marceline, J., Joshi, G. P., & Cho, W. (2023). A quantum-resistant blockchain system: A comparative analysis. *Mathematics*, 11(18), 3947.
8. Michelagnoli, C. (2023). Quantum-resistant Blockchain (Doctoral dissertation, Politecnico di Torino).
9. Zheng, X. (2024). Research on blockchain smart contract technology based on resistance to quantum computing attacks. *Plos one*, 19(5), e0302325.
10. Chauhan, S., Ojha, V. P., Yarahmadian, S., & Carvalho, D. (2023, November). Towards building quantum resistant blockchain. In 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-9). IEEE.
11. Adelusi, B. S., Ojika, F. U., & Uzoka, A. C. (2023). Quantum-Resistant Cryptographic Protocols: Securing Financial Transactions and Protecting Sensitive Business Data in the AI Era.
12. Liu, Y., Zhao, B., Lin, X., Guan, Z., Li, D., Liu, J., ... & Deng, R. H. (2025). Quantum-Resistant Sharding Blockchain and Its Application in Secure Data Transmission. *IEEE Journal on Selected Areas in Communications*.
13. Zhang, P., Wang, L., Wang, W., Fu, K., & Wang, J. (2021). A blockchain system based on quantum-resistant digital signature. *Security and Communication Networks*, 2021(1), 6671648.
14. Unogwu, O. J., Doshi, R., Hiran, K. K., & Mijwil, M. M. (2022). Introduction to quantum-resistant blockchain. In *Advancements in quantum blockchain with real-time applications* (pp. 36-55). IGI Global Scientific Publishing.
15. Sinai, N. K., & In, H. P. (2024). Performance evaluation of a quantum-resistant Blockchain: a comparative study with Secp256k1 and Schnorr. *Quantum Information Processing*, 23(3), 99.
16. Balasubramaniam, A., & B, S. (2023, August). Quantum-resistant Blockchain Cryptography-based Smart City Transactions. In *Proceedings of the 2023 Fifteenth International Conference on Contemporary Computing* (pp. 94-101).
17. Sahu, D. R., Tiwari, H., Tomar, D. S., & Pateriya, R. K. (2024). Quantum-resistant cryptography to prevent from phishing attack exploiting blockchain wallet. In *Sustainable security practices using blockchain, quantum and post-quantum technologies for real time applications* (pp. 171-191). Singapore: Springer Nature Singapore.
18. Muda, I., Santosh, K., Aarif, M., Natrayan, L., Kaliappan, S., & Muthuperumal, S. (2024, July). Innovative Blockchain Protocol for Enhancing Transaction Security and Integrity in Decentralized Financial Ecosystems. In 2024 International Conference on Data Science and Network Security (ICDSNS) (pp. 1-6). IEEE.
19. Zahoor, Q., & De Roest, H. (2024). Quantum-Resistant Blockchain: Preparing for the Future of Cyber Security.
20. Peelam, M. S., & Chamola, V. (2024). Enhancing security using quantum blockchain in consumer IoT networks. *IEEE Transactions on Consumer Electronics*.
21. Kale, M. R., El-Ebiary, Y. A. B., Sathiya, L., Burugari, V. K., Yulduz, E., Muniyandy, E., & Alanazi, R. (2025). Designing Quantum-Resilient Blockchain Frameworks: Enhancing Transactional Security with Quantum Algorithms in Decentralized Ledgers. *International Journal of Advanced Computer Science & Applications*, 16(4).

22. Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE access*, 8, 21091-21116.
23. Umar, A., & Kumar, D. (2024, October). Quantum-Resistant Security Analysis of Blockchain Networks with PoS Consensus. In *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)* (pp. 1-6). IEEE.
24. Verma, R. (2021). The Future of Cryptocurrency: Quantum-Secure Blockchain Protocols. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, 2(4), 11-17.
25. An, H., & Kim, K. (2018, January). QChain: Quantum-resistant and decentralized PKI using blockchain. In *2018 Symposium on Cryptography and Information Security (SCIS 2018)*. IEICE Technical Committee on Information Security.
26. Taj, I., & Adnan, M. (2025). Quantum-Resistant Security Framework for Secure and Scalable IoT-enabled Metaverse Environments. *IEEE Transactions on Consumer Electronics*.
27. Tawfik, M., Abdelhaliem, A. H., & Fathi, I. (2025). Quantum-Resistant Privacy-Preserving IoT Authentication via Zero-Knowledge Proofs and Blockchain Integration. *Statistics, Optimization & Information Computing*, 14(3), 1374-1402.
28. Gong, Y., & Hu, B. J. (2024). A quantum-resistant key management scheme using blockchain in C-V2X. *IEEE Transactions on Intelligent Transportation Systems*.
29. Das, S., Mondal, S., Golder, S. S., Sutradhar, S., Bose, R., & Mondal, H. (2024, December). Quantum-Resistant Security for Healthcare Data: Integrating Lamport n-Times Signatures Scheme with Blockchain Technology. In *2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAIQSA)* (pp. 1-8). IEEE.
30. Shah, K., Ukani, M., & Bhadja, S. (2024, July). A detailed exploration to quantum resistant blockchain technology. In *2024 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)* (pp. 1-6). IEEE.