Amratanshu, 2025, 13:1
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Securing Digital Assets in the Quantum Era: A Comprehensive Approach to Blockchain Wallet Security

Amratanshu
Department of Computer Science and Engineering
Institute of Engineering and Rural Technology, Prayagraj, UP (India)

Abstract- This research addresses the growing need for enhanced security in blockchain wallets, focusing on emerging threats like quantum computing. It proposes a framework to future-proof wallets by integrating post-quantum cryptography (PQC), advanced biometric authentication, and decentralized security. With traditional cryptographic algorithms like RSA and ECC vulnerable to quantum decryption, PQC is essential for securing digital assets long-term. Additionally, biometric techniques, such as fingerprint and facial recognition, offer a robust defense against unauthorized access. The study also explores decentralized security by combining PQC with blockchain's immutable ledger to resist quantum threats. Innovative solutions, such as zero-knowledge proofs (ZKPs) for privacy-preserving biometric authentication and advanced techniques like multi-signature and behavioral biometrics, are examined to strengthen wallet security. A decentralized biometric sharding approach is proposed to protect encrypted biometric data, while context-aware dynamic authentication adjusts security policies based on user behavior. A decentralized recovery system using threshold cryptography is introduced to tackle key recovery. Looking ahead, the paper explores the potential of emerging interfaces like holographic displays and brain-machine interface (BMI) authentication to improve wallet usability and security. This research outlines a comprehensive roadmap for the next generation of blockchain wallets, combining advanced security technologies, energy efficiency, and future-ready features for a seamless, secure digital asset management experience.

Keywords- Blockchain, Hardware Security Modules (HSM), Cryptography, Zero-Knowledge Proofs (ZKPs), Renewable Energy, Biometric Authentication, Quantum Computing, Permissioned Blockchain.

I. INTRODUCTION

1. Background

Blockchain wallet [1] have become essential for managing digital assets, facilitating secure and decentralised transactions in our increasingly digital world. Since the emergence of blockchain technology with Bitcoin in 2008, wallets have evolved from basic cryptocurrency storage tools to complex platforms that support decentralised applications and smart contracts. Early blockchain wallets relied on traditional cryptographic techniques such as RSA and Elliptic Curve Cryptography (ECC) [2] to secure private keys and enable secure transactions. However, the rapid increase in computational power and the rise of quantum computing pose significant threats to these established cryptographic algorithms. The

© 2025 Amratanshu. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

potential for quantum computers to break these algorithms has spurred the need for new security solutions. The evolution of cryptocurrency has introduced new opportunities for financial inclusion, privacy and transparency. However, this has also highlighted the critical need for secure and user-friendly solutions for managing digital assets. Traditional software and hardware wallets, while widely used, are often vulnerable to cyberattacks, physical theft and loss of access due to poor key management. Existing hardware wallets have drawbacks, including reliance on centralised systems for firmware updates, opaque transaction records and complex user interfaces.

2. Problem Statement

Current blockchain wallets face several significant security vulnerabilities Traditional software wallets are susceptible to malware, phishing scams and hacking Although hardware wallets offer improved security with offline storage and transaction signing, they still have limitation These include dependence on centralised systems, opaque transaction records and complex user interface Furthermore, current blockchain wallets often lack robust hardware-based security measures and struggle with interoperability between different currencies and blockchain networks

The most pressing issue is the emerging threat of quantum computing [3-4], which could compromise the cryptographic foundations of current wallets Algorithms like RSA and ECC, which were once considered secure, are vulnerable to decryption by quantum computers This vulnerability exposes sensitive private keys, putting digital assets at risk. Additionally, the increasing sophistication of cyberattacks and the reliance on centralised authentication methods further exacerbate the need for enhanced security measures.

3. Objectives

This research paper presents a comprehensive framework to address the security vulnerabilities of current blockchain wallets, focusing on future-proofing them against emerging threats. The primary objective is to explore and integrate several key innovations:

- **Post-Quantum Cryptography (PQC) [3-4]:** To integrate PQC algorithms, such as lattice-based, hash-based, code-based, and multivariate polynomial cryptosystems, to ensure resilience against quantum computing attacks.
- **Advanced Biometric Authentication:** To integrate advanced biometric techniques, such as multi-signature biometrics and behavioral biometrics, to improve authentication robustness. A decentralised biometric sharding approach will also be explored to protect user privacy. The use of zero-knowledge proofs (ZKPs) [5] for privacy-preserving biometric authentication will be investigated.
- **Decentralised Security Models:** To develop and implement decentralised security mechanisms, including threshold cryptography for key recovery and context-aware dynamic authentication that uses AI to adapt security policies. The study will examine the integration of decentralized identity management frameworks to empower users with more control over their digital identities.
- **Hardware Security Modules (HSMs):** To explore the use of HSMs, such as Trusted Platform Modules (TPMs), for secure key storage and cryptographic operations. The integration of HSMs with Permissioned Blockchain (PB) [6] technologies like Hyperledger Fabric will be evaluated.
- **Emerging Technologies:** To evaluate emerging technologies, such as holographic displays and brain-machine interfaces (BMI), to improve usability and security. The design of energy-efficient hardware wallets will also be considered.

By combining these elements, the research seeks to create a secure, scalable, and user-friendly platform for managing digital assets in a quantum-enabled future.

4. Significance of the Study

The importance of future-proofing blockchain wallets cannot be overstated As digital assets become more integrated into the global financial system, ensuring their security is essential The integration of PQC, biometric authentication [7] ,

and decentralised security [8] is critical for safeguarding digital assets against evolving threats, including quantum computing This research provides a roadmap for the next generation of blockchain wallets by addressing key challenges of security, privacy, and usability. The Block Secure Ledger, a hardware wallet driven by blockchain technology, is an example of how cutting-edge security features, user-friendly design, and effective operation can be combined.

The study's findings will help in:

- Enhancing the security of digital assets by incorporating quantum-resistant cryptography and advanced biometric authentication.
- Protecting users' privacy through the implementation of decentralised security measures and privacy-preserving technologies.
- Improving the usability of blockchain wallets through intuitive interfaces and advanced authentication mechanisms.
- Ensuring the sustainability of digital asset management with energy-efficient design and renewable energy options.
- Promoting interoperability between different blockchain platforms and digital currencies.
- Providing a framework for future research and development in the area of blockchain wallet security.

This research addresses the critical vulnerabilities of traditional wallets, offering a solution that is both secure and user-friendly, and ensuring the long-term security and scalability of blockchain technology

II. LITERATURE REVIEW

1. Overview of Blockchain Wallet Security

Current blockchain wallets rely on cryptographic techniques to secure private keys and enable secure transactions. The most commonly used methods include RSA and Elliptic Curve Cryptography (ECC) [2] These techniques have been fundamental to securing digital assets, ensuring the confidentiality and integrity of transactions. However, these methods have inherent limitations, particularly in the face of emerging threats

- RSA, while widely used, is vulnerable to attacks from increasingly powerful computing systems and requires continuously increasing key sizes, which can be inefficient for resource-constrained devices.
- ECC, although more efficient than RSA, is also at risk from quantum computing. Both RSA and ECC could potentially be decrypted by quantum computers, exposing sensitive private keys and jeopardizing the security of digital assets
- Traditional hardware wallets [9] offer improved security with offline storage, but they still depend on centralised systems for firmware updates and have complex user interfaces.
- Software wallets [9] are vulnerable to malware and hacking The security of these wallets depends on the security of the device they are installed on these limitations highlight the need for more robust security measures to protect blockchain wallets from both existing and future threats.

A future-proof blockchain wallet is more than just a storage device; it is a comprehensive system that combines the benefits of advanced cryptography, biometric authentication, decentralised technologies, and user-centric design to provide a secure, private, and user-friendly platform for managing digital assets in an era of rapid technological advancement It represents a significant step forward in blockchain security, promising to transform how digital assets are managed and safeguarded in the coming years

2. Quantum Computing and Cryptography

Quantum computing poses a significant threat to the security of current cryptographic systems Quantum computers leverage the principles of quantum mechanics to perform complex calculations exponentially faster than classical computers. This capability threatens to render traditional cryptographic algorithms like RSA and ECC obsolete.

- Quantum computers could potentially decrypt private keys, undermining the security of blockchain wallets.

- The development of post-quantum cryptography (PQC) [4] is essential to safeguard against these threats.
- PQC algorithms are designed to resist attacks from both classical and quantum computers, ensuring the long-term security of digital assets.

The emergence of quantum computing requires a shift from traditional cryptography to quantum-resistant solutions to maintain the security of blockchain systems.

3. Advances in Biometric Authentication [7]

Biometric authentication offers an additional layer of security by verifying a user's identity based on unique biological traits. Traditional biometric methods like fingerprint and facial recognition have been integrated into some blockchain applications. However, these methods can be vulnerable to spoofing attacks.

- Multi-signature biometrics are being developed to enhance the security of authentication by requiring multiple biometric verifications.
- Behavioral biometrics analyse unique patterns in user behaviour, such as typing speed and mouse movements, offering an additional layer of security against unauthorized access.
- Zero-knowledge proofs (ZKPs) [5] are a way of enhancing biometric authentication by ensuring sensitive biometric data is not exposed during the authentication process.
- Decentralized biometric sharding is a privacy-preserving technique that distributes encrypted biometric data across blockchain nodes to maintain privacy and security These advanced techniques improve both the security and usability of blockchain wallets, making it more difficult for unauthorised users to gain access.

4. Decentralized Security in Blockchain Ecosystems [7]

Decentralized security models are increasingly important in the blockchain ecosystem to reduce reliance on centralised authorities. Blockchain itself provides a decentralized and immutable ledger, which improves transparency and security However, implementing truly decentralized security mechanisms requires further innovation.

- Permissioned Blockchains (PBs), like Hyperledger Fabric, offer a way to control network access and increase scalability These networks require participants to have specific permissions, adding a layer of security.
- Threshold cryptography provides a secure solution for key recovery, mitigating the risks of key loss by distributing key shares among multiple parties.
- Decentralized identity management frameworks provide users with greater control over their digital identities and authentication processes.
- Context-aware dynamic authentication utilises AI to adjust security policies in real time based on user behaviour and environmental factors.

These decentralized methods aim to enhance the security of blockchain systems while also addressing privacy and scalability issues.

III. MATERIALS AND METHODS

1. Post-Quantum Cryptography (PQC) [4]

This study will analyse and integrate various post-quantum cryptographic techniques into blockchain wallet systems. The primary goal is to ensure resilience against quantum computing attacks.

- Lattice-based cryptography [4] will be analysed for its suitability in securing blockchain wallets due to its strong theoretical foundations and its resistance to quantum attacks.
- Hash-based cryptography [4] which is based on the properties of cryptographic hash functions, will be considered for its security and efficiency in blockchain applications.
- Code-based cryptography [4] which uses algebraic codes for encryption and decryption, will be evaluated for its effectiveness against quantum adversaries.
- Multivariate polynomial cryptosystems, which are based on systems of multivariate polynomial equations, will be explored for their applicability in securing blockchain wallets.
- Key selection criteria will include computational efficiency, security against quantum attacks, and compatibility with blockchain frameworks.

- Experimental simulations will be conducted to test the performance of PQC algorithms in terms of encryption, decryption, and signing speeds within a blockchain ecosystem.

This analysis aims to identify the most suitable PQC algorithms for integration into blockchain wallets, providing a foundation for future quantum-resistant systems.

2. Biometric Authentication Techniques [7]

This research will evaluate both traditional and emerging biometric authentication methods for their effectiveness and suitability in blockchain wallets.

- Traditional biometrics, such as fingerprint and facial recognition, will be assessed for their ease of integration into hardware wallets and their resistance to spoofing attacks.
- Advanced biometric techniques, including behavioral biometrics and multi-signature biometric authentication [7,9], will be explored to enhance authentication robustness and usability.
- Privacy-preserving technologies, such as zero-knowledge proofs (ZKPs), will be incorporated to enhance biometric authentication by ensuring that sensitive biometric data is not exposed during authentication processes.
- A decentralized biometric sharding approach [9] will be implemented, where encrypted biometric data is fragmented and distributed across blockchain nodes. This will improve both privacy and security by eliminating a single point of failure.
- The integration of these methods aims to offer a seamless user experience with enhanced security against unauthorized access.

3. Decentralized Security Framework

This study will implement a decentralized security framework to complement blockchain's inherent immutability and transparency.

- Threshold cryptography will be applied to develop a decentralized key recovery system, mitigating the risks associated with private key loss.
- Decentralized identity management frameworks will be explored to establish user-centric control over authentication and key recovery processes.
- Context-aware dynamic authentication will be introduced as a method for real-time security adaptation. This approach will leverage AI to analyse user behaviour and environmental conditions to adjust security policies dynamically.
- The research will also explore the use of Hardware Security Modules (HSMs) such as Trusted Platform Modules (TPMs) for secure key storage and cryptographic operations in blockchain wallets
- The integration of HSMs with Permissioned Blockchain (PB) [6] technologies like Hyperledger Fabric will also be explored.

This decentralized approach ensures that no single entity controls the security mechanisms, thereby increasing the robustness and reliability of the system.

4. Innovative Authentication Mechanisms

This research will explore innovative authentication mechanisms to enhance both security and usability in blockchain wallets.

- Context-aware dynamic authentication will be implemented to adapt security policies in real time. This will involve leveraging AI to analyse user behaviour and environmental conditions to dynamically adjust security measures.
- The integration of AI and zero-knowledge proofs (ZKPs) [5] will be explored to create robust privacy-preserving authentication mechanisms.
- A conceptual analysis of future interfaces, such as holographic displays and brain-machine interfaces (BMI) [10] for blockchain wallets will be carried out to evaluate their usability and energy efficiency.

This analysis will focus on the feasibility of these technologies and their potential to provide seamless and secure user experiences. The integration of these technologies will provide a

more robust, user-friendly, and secure system for managing digital assets.

IV. ARCHITECTURE OF THE FUTURE-PROOF BLOCKCHAIN WALLET AND WORKFLOW

The core architecture will feature a hardware security module (HSM), such as a Trusted Platform Module (TPM), to provide a secure root of trust for key generation and storage, and for cryptographic operations This hardware component will be encased in a tamper-resistant material to protect it from physical attacks The wallet will use post-quantum cryptography (PQC) algorithms to protect against quantum computing threats, alongside traditional cryptographic methods like elliptic curve cryptography (ECC) For authentication, it will incorporate biometric authentication, potentially including multi-signature biometrics and behavioral biometrics, with zero-knowledge proofs (ZKPs) and decentralized biometric sharding to protect user data.

The wallet's workflow will involve secure enrollment processes, typically with a certificate authority, and secure transaction signing using the TPM. The user will interact with the device via a user-friendly interface, possibly including a touchscreen, and more futuristic interfaces such as holographic displays or brain-machine interfaces could also be integrated. All transactions will be recorded on a decentralized ledger using blockchain technology. For security and privacy, the system will employ context-aware dynamic authentication, adjusting security protocols based on real-time data, and will leverage decentralized identity management for user control over their digital identities. Additionally, decentralized key recovery systems using threshold cryptography will mitigate the risks of key loss The device will also include features like offline transaction signing to minimise exposure to online threats, support multi-currency portfolios, and offer a secure firmware update mechanism. The wallet’s design will focus on usability and accessibility, ensuring that both technical and non-technical users can easily navigate the system The use of energy harvesting technologies, such as solar panels, is also considered for greater sustainability.

V. RESULTS AND VALIDATION

1. Performance Evaluation of PQC Algorithms

The evaluation of Post-Quantum Cryptography (PQC) algorithms will focus on their efficiency in the context of a blockchain wallet environment. This includes measuring the time taken for:

- **Encryption:** The speed at which data can be encrypted using PQC algorithms is a key factor, as this directly impacts the performance of secure data storage and communication.
- **Decryption:** The efficiency of decryption processes will also be evaluated, as this is essential for accessing encrypted data in a timely manner.
- **Signing:** The speed at which transactions can be signed using PQC algorithms is crucial, as it will impact the user experience when making transactions.
- **Computational Efficiency:** Key selection criteria will include an assessment of the computational efficiency of the different PQC methods.
- **Compatibility:** PQC algorithms will be assessed for compatibility with blockchain frameworks.

2. Biometric Authentication Performance

The performance of biometric authentication methods will be assessed across several dimensions:

- **Resistance to Spoofing Attacks:** The robustness of biometric methods against spoofing attempts will be tested. This includes evaluating the ability of the system to distinguish between genuine biometric data and fake data. Both traditional biometric systems like fingerprint and facial recognition, and emerging techniques like behavioural biometrics and multi-signature biometric authentication will be assessed.
- **User Convenience:** The ease of use of biometric methods will be evaluated. The goal is to ensure that the authentication process is both secure and convenient for the user.

- **Privacy:** The integration of privacy-preserving technologies like zero-knowledge proofs (ZKPs) will enhance biometric authentication by ensuring sensitive biometric data is not exposed during the authentication process.
- Decentralised biometric sharding will be used to distribute encrypted biometric data across blockchain nodes to maintain privacy and security

3. Security Analysis

A thorough security analysis will be conducted to assess the resilience of the future-proof blockchain wallet against various threats:

- **Quantum Attacks:** The primary focus will be on the wallet's ability to withstand quantum computing attacks. The integration of post-quantum cryptography (PQC) will be rigorously tested to ensure its effectiveness.
- **Cyber Threats:** The wallet's resistance to traditional cyber threats, such as malware, phishing scams, and hacking, will be assessed.
- **Physical Attacks:** The tamper-resistant design of the wallet will be evaluated for its ability to protect against physical attacks, such as attempts to access the device's internal components. The hardware security module (HSM) [11], specifically a Trusted Platform Module (TPM), will play a key role in providing tamper-proof protection for the wallet.
- **Side Channel Attacks:** The resistance of the HSM to side-channel attacks will be assessed.
- **Malware Attacks:** The trusted boot mechanisms will protect against malware attacks23

4. Comparative Analysis

The proposed future-proof blockchain wallet will be compared against traditional blockchain wallets to highlight its advantages:

- **Security:** The security of the new wallet will be compared with that of traditional software and hardware wallets The vulnerabilities of traditional wallets to cyber-attacks, malware, phishing scams, and hacking will be highlighted.
- **Usability:** The user experience and ease of use of the new wallet will be compared to existing wallet solutions.
- **Quantum Resistance:** The ability of traditional wallets to protect against quantum computing attacks is minimal. The new wallet with PQC will be contrasted against traditional methods.
- **Decentralization:** The use of on-device blockchain nodes will be used to highlight the enhanced decentralization and autonomy of the proposed system.

By addressing the current challenges and anticipating future threats, the proposed blockchain wallet aims to set a new standard for the industry, ensuring long-term security, scalability, and a user-centric design

Future Implications

Adoption of Quantum-Safe Technologies: The integration of post-quantum cryptography (PQC) is crucial for the long-term security of blockchain wallets. As quantum computing advances, traditional cryptographic algorithms such as RSA and ECC become vulnerable, necessitating the shift to quantum-resistant algorithms. The adoption of PQC ensures that digital assets remain secure against quantum attacks, making wallets resilient in a quantum-enabled future Examples of PQC algorithms include lattice-based cryptography (e.g., CRYSTALS-Dilithium), which are designed to withstand quantum threats.

- Role of Emerging Interfaces: The evolution of blockchain wallets includes the integration of advanced user interfaces.
- Holographic Displays: These offer a secure way to review transaction details, eliminating the risk of physical screen tampering. Holographic displays provide a tamper-proof and secure interface for user interaction.
- Brain-Machine Interfaces (BMI): BMI authentication is being explored as a futuristic and highly secure authentication mechanism, allowing users to authenticate wallets using specific thought patterns or brainwave signatures.

VI. CONCLUSION

The Block Secure Ledger is a significant step forward in hardware wallet technology, combining blockchain's decentralised architecture with strong hardware encryption, using a Hardware Security Module (HSM), such as a Trusted Platform Module (TPM), to ensure private keys are never exposed This is combined with post-quantum cryptography (PQC) for future security against quantum computing threats, and advanced biometric authentication, while offering offline transaction signing Future developments should focus on optimising PQC, incorporating emerging biometrics like AI-powered behavioural biometrics, enhancing decentralised security, prioritising user experience with interfaces like holographic displays, adding energy-efficient technologies, implementing on-device blockchain nodes, and integrating federated learning and decentralised identity systems

REFERENCES

1. Popchev, Ivan & Radeva, Irina & Dimitrova, Miroslava. (2023). Towards Blockchain Wallets Classification and Implementation. 10.1109/ICAI58806.2023.10339101.
2. Hankerson, D., Menezes, A.J. and Vanstone, S., 2006. Guide to elliptic curve cryptography. Springer Science & Business Media.
3. Kokare, Priyanka & Vora, Deepali & Patil, Shruti & Kotecha, Ketan & Khairnar, Vaishali & Choudhury, Tanupriya & Kulkarni, Ambarish. (2024). Post Quantum Cryptography: A survey of Past and Future.
4. D. Bellizia et al., "Post-Quantum Cryptography: Challenges and Opportunities for Robust and Secure HW Design," 2021 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), Athens, Greece, 2021, pp. 1-6, doi: 10.1109/DFT52944.2021.9568301.
5. Zhou, Y., Wei, Z., Ma, S., Tang, H. (2022). Overview of Zero-Knowledge Proof and Its Applications in Blockchain. In: Sun, Y., Cai, L., Wang, W., Song, X., Lu, Z. (eds) Blockchain Technology and Application. CBCC 2022. Communications in Computer and Information Science, vol 1736. Springer, Singapore. https://doi.org/10.1007/978-981-19-8877-6_5
6. Vittorio Capocasale, Danilo Gotta, Guido Perboli, Comparative analysis of permissioned blockchain frameworks for industrial applications, Blockchain: Research and Applications, Volume 4, Issue 1,2023,100113, ISSN 2096-7209, https://doi.org/10.1016/j.bcra.2022.100113.
7. Jain, A.K., Ross, A. (2008). Introduction to Biometrics. In: Jain, A.K., Flynn, P., Ross, A.A. (eds) Handbook of Biometrics. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-71041-9_1
8. Wang, H., Wang, Y., Cao, Z., Li, Z., Xiong, G. (2019). An Overview of Blockchain Security Analysis. In: Yun, X., et al. Cyber Security. CNCERT 2018. Communications in Computer and Information Science, vol 970. Springer, Singapore. https://doi.org/10.1007/978-981-13-6621-5_5
9. Sharma, S., Saini, A., & Chaudhury, S. (2024). Multimodal biometric user authentication using improved decentralized fuzzy vault scheme based on Blockchain network. Journal of Information Security and Applications, 82, Article 103740. https://doi.org/10.1016/j.jisa.2024.103740
10. Abdullah Ayub Khan, Asif Ali Laghari, Aftab Ahmed Shaikh, Mazhar Ali Dootio, Vania V. Estrela, Ricardo Tadeu Lopes, A blockchain security module for brain-computer interface (BCI) with Multimedia Life Cycle Framework (MLCF), Neuroscience Informatics, Volume 2, Issue 1, 2022, 100030, ISSN 2772-5286, https://doi.org/10.1016/j.neuri.2021.100030.
11. Sommerhalder, Maria. (2023). Hardware Security Module. 10.1007/978-3-031-33386-6_16.