iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78497

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Design of a Secure Blockchain-Based Cryptocurrency Wallet with Offline Transaction Capability

Shariff Usman[1], Tiruveedhi K.V.V. Sai Sriram[2], Thati Mithra[3]
Department of Computer Applications, Aditya University, Surampalem, India,

Abstract: ***Blockchain technology has transformed digital financial systems by enabling decentralized and secure transactions. Despite these advancements, cryptocurrency wallets remain a critical point of vulnerability due to their dependence on continuous internet connectivity and exposure to cyber threats. This paper proposes a secure cryptocurrency wallet architecture that incorporates offline transaction signing and robust cryptographic mechanisms to mitigate security risks. The system utilizes public-key cryptography, hashing algorithms, and encryption techniques to ensure confidentiality, integrity, and authentication of transactions. The offline signing mechanism enables secure transaction authorization without exposing private keys to online environments. Furthermore, the proposed system enhances key management through encrypted storage and secure access protocols. The results demonstrate that the proposed architecture significantly reduces attack vectors and improves overall system resilience, making it a reliable solution for secure cryptocurrency transactions.***

Index Terms: ***Blockchain Technology, Cryptocurrency Security, Digital Wallet, Public-Key Cryptography, Encryption, Hash Functions, Transaction Authentication, Decentralized Systems***

I. INTRODUCTION

The advancement of digital technologies has led to the emergence of cryptocurrencies as a decentralized form of financial exchange. Cryptocurrencies such as Bitcoin and Ethereum operate on blockchain technology, which ensures transparency, immutability, and secure peer-to-peer transactions without the involvement of centralized authorities. This innovation has significantly transformed the way digital transactions are performed and managed. A cryptocurrency wallet is an essential component of the blockchain ecosystem, enabling users to store, manage, and transfer their digital assets. These wallets function using cryptographic mechanisms, primarily involving public and private keys. The private key is used to authorize transactions, while the public key is used to verify and receive funds. Therefore, the security of the wallet is directly dependent on the protection of these cryptographic keys.

Despite the benefits of blockchain technology, cryptocurrency wallets are still vulnerable to various security threats. Many existing wallets operate in online environments, making them susceptible to phishing attacks, malware, hacking attempts, and unauthorized access. These threats can lead to the exposure of private keys and result in significant financial losses, which are often irreversible due to the nature of blockchain transactions. To improve security, several wallet solutions have introduced mechanisms such as encryption, multi-factor authentication, and hardware-based storage. However, these solutions still rely heavily on internet connectivity during transaction processing, which creates potential risks. The exposure of private keys during online transactions remains a major concern in existing systems.

In order to address these challenges, there is a need for a more secure wallet architecture that minimizes the risks associated with online environments. This paper proposes a blockchain-based cryptocurrency wallet system that incorporates offline transaction capability. By enabling transactions to be signed offline, the system reduces the chances of private key exposure and enhances overall security.

The proposed system integrates advanced cryptographic techniques such as public-key cryptography, secure hash functions, and encryption methods to ensure confidentiality, integrity, and authentication. Additionally, it includes a secure key management mechanism that protects user credentials and prevents unauthorized access.

The primary objective of this research is to design a secure and efficient cryptocurrency wallet system that enhances user safety while maintaining usability. The proposed approach aims to overcome the limitations of existing wallets by providing improved security features and reducing vulnerability to cyber-attacks, thereby increasing trust in blockchain-based financial systems.

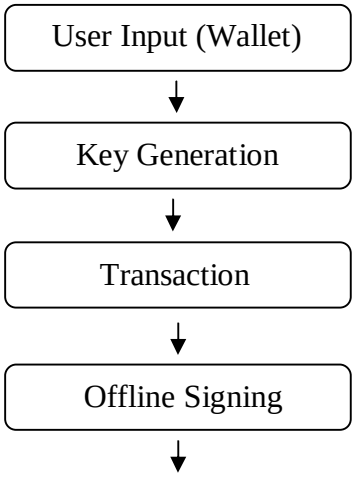
II. LITERATURE REVIEW

Several studies have explored the design and security of cryptocurrency wallets within blockchain-based systems. Early work by Nakamoto [1] introduced the concept of decentralized digital currency, highlighting the importance of cryptographic security in financial transactions. Subsequent research has focused on improving wallet security through various mechanisms such as encryption, authentication, and secure key management. Popular wallet applications such as MetaMask, Trust Wallet, and Electrum provide essential functionalities including key storage, transaction execution, and blockchain interaction; however, they are primarily dependent on internet connectivity, which exposes them to potential cyber threats. Studies have identified common vulnerabilities in these wallets, including phishing attacks, malware injection, and unauthorized access to private keys [2]. To mitigate these risks, researchers have proposed hardware wallets and multi-factor authentication systems, which enhance security but may reduce usability and accessibility [3]. Additionally, several approaches utilize encryption algorithms and secure hash functions to protect sensitive data and ensure transaction integrity [4]. Despite these advancements, the exposure of private keys during online transaction processing remains a significant limitation in existing systems. Therefore, recent research emphasizes the need for improved wallet architectures that incorporate offline transaction mechanisms and enhanced security models. The proposed system in this paper builds upon these existing approaches by integrating offline transaction signing and secure key management techniques to minimize vulnerabilities and improve overall system reliability.

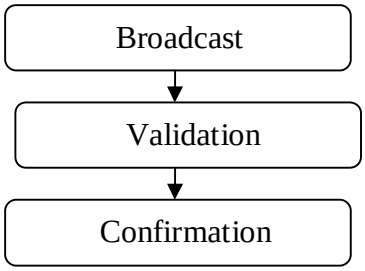
III. SYSTEM ARCHITECTURE

The proposed system is designed as a secure blockchain-based cryptocurrency wallet with offline transaction capability, consisting of multiple interconnected modules that ensure secure key management, transaction processing, and interaction with the blockchain network. The architecture is divided into three major components: the user interface layer, the wallet processing layer, and the blockchain network layer. The process begins with the user interacting with the wallet application through a user-friendly interface, where inputs such as transaction details are provided. The system then performs key generation, where a pair of cryptographic keys, namely the public key and private key, is created. The private key is securely stored using encryption techniques, while the public key is used to generate the wallet address. Once the transaction details are entered, the system generates transaction data, which is then passed to the offline transaction signing module. In this module, the transaction is signed using the private key in an isolated offline environment, ensuring that sensitive information is not exposed to online threats. This approach significantly enhances the security of the system by preventing unauthorized access to private keys. After the transaction is signed, it is transferred to the online environment for broadcasting to the blockchain network. The transaction is then verified by network nodes using cryptographic validation techniques and is recorded in the distributed ledger. A consensus algorithm ensures agreement among nodes before confirming the transaction. The architecture also includes an encryption and security module that implements advanced cryptographic techniques such as Advanced Encryption Standard (AES) and secure hash algorithms to protect user data and maintain data integrity. This module ensures that all sensitive information, including private keys and transaction details, is securely handled within the system. Finally, the blockchain network layer processes the transaction through validation, consensus, and confirmation stages, after which the transaction is permanently stored in the distributed ledger. The overall architecture ensures a secure, reliable, and efficient cryptocurrency wallet system by combining offline transaction signing with robust cryptographic security mechanisms.

Fig. 1. Proposed System Architecture



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com



IV. PROPOSED METHODOLOGY

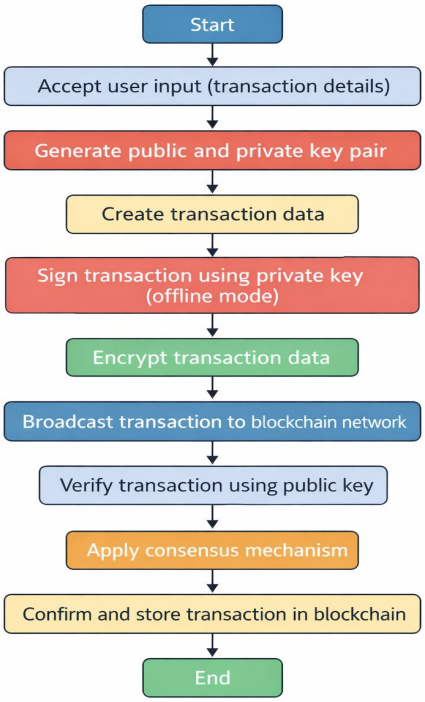
The proposed methodology focuses on developing a secure cryptocurrency wallet system that enhances transaction safety through offline signing and advanced cryptographic techniques. The system follows a structured workflow beginning with user input, where transaction details such as recipient address and amount are provided through the wallet interface. Upon receiving the input, the system generates a pair of cryptographic keys consisting of a public key and a private key. The private key is securely stored using encryption techniques, while the public key is used for transaction verification.

Once the keys are generated, the system proceeds to create transaction data, which includes essential details required for processing the transaction. This transaction data is then transferred to the offline signing module, where the transaction is signed using the private key in an isolated offline environment. This step ensures that sensitive key information is not exposed to online threats, thereby improving the overall security of the system.

After successful signing, the transaction is encrypted and broadcasted to the blockchain network. The network nodes then verify the transaction using cryptographic validation techniques. A consensus mechanism is applied to confirm the transaction, ensuring agreement among participating nodes. Once verified, the transaction is permanently recorded in the distributed ledger.

The proposed methodology integrates security mechanisms such as encryption, digital signatures, and secure key management to protect user data and ensure transaction integrity. By incorporating offline transaction capability, the system minimizes vulnerabilities associated with traditional online wallets and provides a secure and efficient solution for cryptocurrency transactions.

Fig. 2. Proposed Methodology Flow Diagram



V. CONCLUSION

This paper presented a secure blockchain-based cryptocurrency wallet system with offline transaction capability. The proposed system enhances the security of digital transactions by protecting private keys and minimizing exposure to online threats. By incorporating advanced cryptographic techniques such as public-key cryptography, encryption, and digital signatures, the system ensures data confidentiality, integrity, and authentication.

The introduction of offline transaction signing significantly reduces the risk of cyber-attacks, including phishing and unauthorized access. The proposed architecture provides a reliable and efficient solution for secure cryptocurrency transactions while maintaining usability. Overall, the system improves trust and security in blockchain-based financial systems.

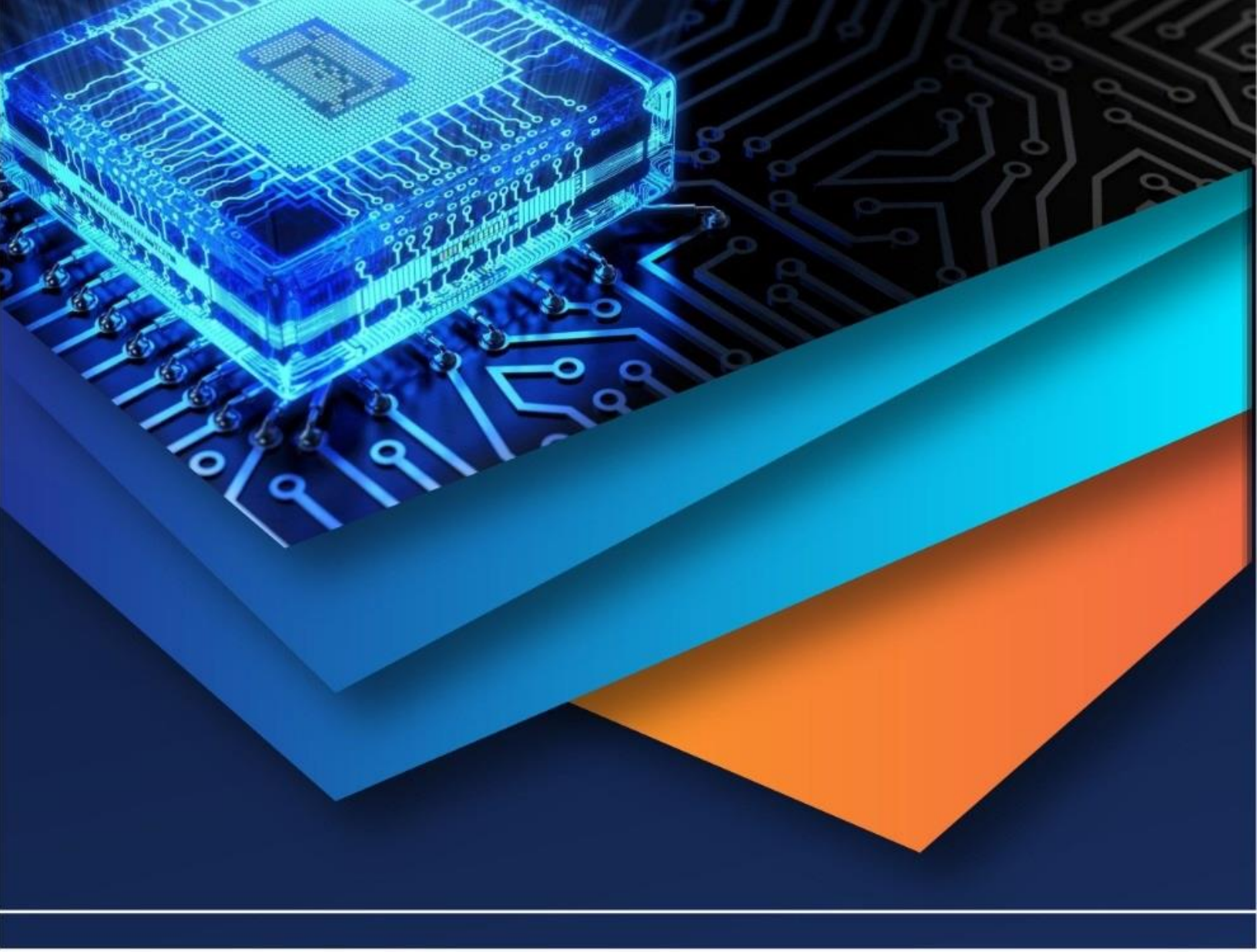
Future work can focus on integrating advanced authentication mechanisms such as biometric verification and multi-factor authentication, as well as improving scalability and compatibility with various blockchain platforms.

VI. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the Department of Computer Applications, Aditya University, for providing the necessary support and resources to carry out this research work. The authors also thank the faculty members and guides for their valuable guidance and encouragement throughout the development of this paper.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
[2] V. Buterin, “Ethereum Whitepaper,” 2015. [Online]. Available: https://ethereum.org
[3] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 2nd ed., Sebastopol, CA, USA: O’Reilly Media, 2017.
[4] NIST, “Secure Hash Standard (SHS),” FIPS PUB 180-4, Aug. 2015.
[5] NIST, “Advanced Encryption Standard (AES),” FIPS PUB 197, Nov. 2001.
[6] D. Boneh and V. Shoup, A Graduate Course in Applied Cryptography, 2020.
[7] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain Technology: Beyond Bitcoin,” Applied Innovation Review, no. 2, pp. 6–19, 2016.
[8] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” Ethereum Project Yellow Paper, 2014.
[9] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.
[10] J. Bonneau et al., “SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies,” in Proc. IEEE Symposium on Security and Privacy, 2015, pp. 104–121.
[11] MetaMask Official Website. [Online]. Available: https://metamask.io
[12] Trust Wallet Official Website. [Online]. Available: https://trustwallet.com



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY