International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

E-Wallet Security using Blockchain Technology

K.P. Sangeetha
Assistant Professor
Cyber Security Department ACS
College of Engineering 207,
Kambipura, Mysore road, Kengeri
Hobli, Bengaluru-560074
kpsangeetha20@gmail.com

Gunavathi C
Bachelor of Engineering
Student
Cyber Security Department ACS
College of Engineering 207,
Kambipur ,Mysure road
Kengeri Hobli,
Bengaluru-560074
gunavathic752@gmail.com

Harshitha N
Bachelor of Engineering
Student
Cyber Security Department ACS
College of Engineering 207,
Kambipur,Mysore road
Kengeri Hobli,
Bengaluru-560074
harshitha04nagraj@gmail.com

Veena AH
Bachelor of Engineering
Student
Cyber Security Department ACS
College of Engineering 207,
Kambipura, Mysore road,
Kengeri Hobli ,
Bengaluru-560074
veenayadav7975@gmail.com

***Abstract* — Traditional wallets and centralised payment apps often face security risks like hacking, phishing, and unauthorised data sharing. A familiar example is the frequent online fraud through UPI and mobile wallets in India, where fake payment links and OTP scams have led to thousands of users losing money. These cases show how centralised control and weak transparency can be exploited. Hardware-based methods also carry risks, such as device theft and tampering. To solve these issues, the system introduces a secure e-wallet built on blockchain technology. With decentralisation, immutability, and transparent verification, blockchain ensures tamper-proof, trustworthy, and secure financial transactions for users.**

I. INTRODUCTION

In the present digital age, financial transactions are swiftly moving away from traditional cash-based methods toward online and mobile payment platforms. This transformation is driven by increasing demands for convenience, speed, and accessibility in daily financial activities. Among the most impactful innovations are electronic wallets (e-wallets) - applications that allow users to securely hold funds, make payments, and manage their financial transactions.Popular e-wallets like Paytm, Google Pay, and PayPal have revolutionized money handling by allowing instant, contactless transactions.

However, despite their convenience, security and privacy remain major concerns in conventional e-wallet systems. Most of these platforms operate on centralised architectures, meaning that all user and transaction data are stored on a single central server. This centralization leads to risks like data breaches, unauthorized access, and system failures.

Once a hacker compromises the central database, sensitive financial data of millions of users can be exposed or altered. Moreover, issues like fraudulent transactions, data manipulation, and lack of transparency weaken user trust in digital payment systems.

Blockchain technology provides an innovative approach to overcoming these challenges. Blockchai works like a shared digital ledger which records all the transaction,making sure that data is secure,transparent and difficult to tamper.Each transaction is securely encrypted, timestamped, and stored within a block linked to previous transactions, forming a continuous and verifiable chain. By removing the advantage for third-parties such as government and bank, this decentralized framework boosts security, improves transparency, and promotes trust within financial systems.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

A. *PROBLEM STATEMENT*

Despite the advantages of digital wallets, current systems face the following challenges:

- Centralized storage systems lead to single points of failure, leaving them susceptible to data breaches and cyberattacks.
- These systems mainly undergo limited transparency and restricted user control over sensitive financial data.
- Vulnerability to cyberattacks, phishing, and fraudulent transactions.
- Dependence on third-party intermediaries for validation and trust management.

B. *OBJECTIVES*

The main focus of this study, named 'Secure E-Wallet Using Blockchain,' is the development and implementation of a blockchain-powered digital wallet that guarantees security, transparency, and immutability in financial transactions. The detailed goals of the research include :

1. To develop a decentralized wallet architecture with the help of blockchain for secure transactions.
2. To employ cryptographic mechanisms to maintain data privacy and be free from unauthorized access.
3. To integrate wallet security through a combination of hot and cold wallet features.
4. To eliminate central authority dependency and establish user-controlled authentication.
5. To evaluate the proposed model's performance and security against traditional systems.

To summarize,this study aims to design a next-generation secure e-wallet that utilizes blockchain's decentralized framework and cryptographic mechanisms, integrating blockchain technology with enhanced wallet security features, the system promotes user confidence, improves transparency, and enhances the robustness of digital payment systems.

II. LITERATURE REVIEW

Mitawa [1] highlights that the rise in cyberattacks and fraudulent activities within payment systems has created an urgent demand for reliable solutions. Their research emphasizes blockchain's immutability a crucial element in minimizing fraud, since transactions recorded on the blockchain are permanent and cannot be altered surreptitiously. This feature establishes a robust foundation of trust, especially for sensitive financial operations.

Yadav et al. [4] explore the use of cryptocurrency wallets in the banking sector, showing that blockchain technology improves operational efficiency while mitigating identity-based threats such as phishing and SIM-swapping. Their study suggests that blockchain-based wallets maintain the user-friendly convenience typical of mobile banking while simultaneously providing stronger security measures. In contrast to Mitawa , Yadav et al. place greater emphasis on practical implementation and real-world usability alongside robust security in financial services.

Bui-Huu et al. [3] examine the rapid adoption of e-wallets during the COVID-19 pandemic. While usage increased dramatically, they observed a corresponding rise in financial crimes, indicating that blockchain alone cannot prevent all risks. Their work highlights the importance of integrating fraud detection mechanisms with blockchain-based systems. This identifies a critical gap in many existing e-wallet solutions: security measures beyond immutability, such as real-time monitoring and anomaly detection.

Guo and Yu [4] offer a detailed review of blockchain security frameworks and consensus mechanisms, tracing their development from Bitcoin to Ethereum. They demonstrate that blockchain's security is well-established, yet also highlight ongoing issues such as scalability, transaction throughput, and complexity of integration. This represents a departure from earlier studies by Mitawa , which mainly explores the theoretical security advantages of immutability without considering practical deployment challenges.

Nowroozi et al. [5] propose a wallet design that enhances privacy using homomorphic encryption, while maintaining usability through cloud integration. Their approach demonstrates that privacy-preserving techniques can be combined with blockchain wallets without sacrificing performance. This highlights a gap in many current e-wallet systems, which often prioritize either security or convenience, but not both.

Le and Hsu [6] systematically analyze blockchain's properties, including decentralization and auditability. Their study confirms that blockchain is suitable for trust-

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

sensitive environments but cautions that challenges like large-scale adoption and interoperability remain unresolved. This supports the argument that while blockchain strengthens security, additional innovation is needed to make it fully practical for mass deployment.

III. METHODOLOGY

A. *SYSTEM ARCHITECTURE*

The proposed secure e-wallet system is structured into four primary layers:

1. **User Interface Layer (Frontend):**
   This layer delivers the interface enabling user interaction with the system. Developed using HTML, CSS, and JavaScript, it allows users to create wallets, check balances, transfer funds, and view transaction histories with ease and clarity.
2. **Application Layer (Backend):**
   Built with Node.js, this backend layer manages user requests, processes transactions, and handles communication with the blockchain network to ensure smooth operation.
3. **Blockchain Layer:**
   This core layer is deployed on the Ethereum blockchain. It maintains a shared digital ledger where every transaction is securely recorded as an immutable block, ensuring data integrity and transparency.
4. **Database Layer :**
   Some non-critical information such as user profiles or interface preferences may be stored off-chain in a secure Firebase cloud. However, sensitive financial and transaction data remain entirely on the blockchain for maximum integrity.

B. ALGORITHM USED

SHA-256 (Secure Hash Algorithm):Used to ensure data integrity by generating a fixed-size hash for each transaction.Any change in input data results in a completely different hash, preventing tampering.

Ethereum Blockchain**:** Smart contracts are self-executing programs on blockchain that immediately enforce agreed upon terms and conditions, enabling transaction processing without any need.

Smart Contracts (Solidity):Self-executing code that manages fund transfers, transaction validation, and wallet operations.Eliminates human intervention, decreasing the impact of fraud or manipulation.

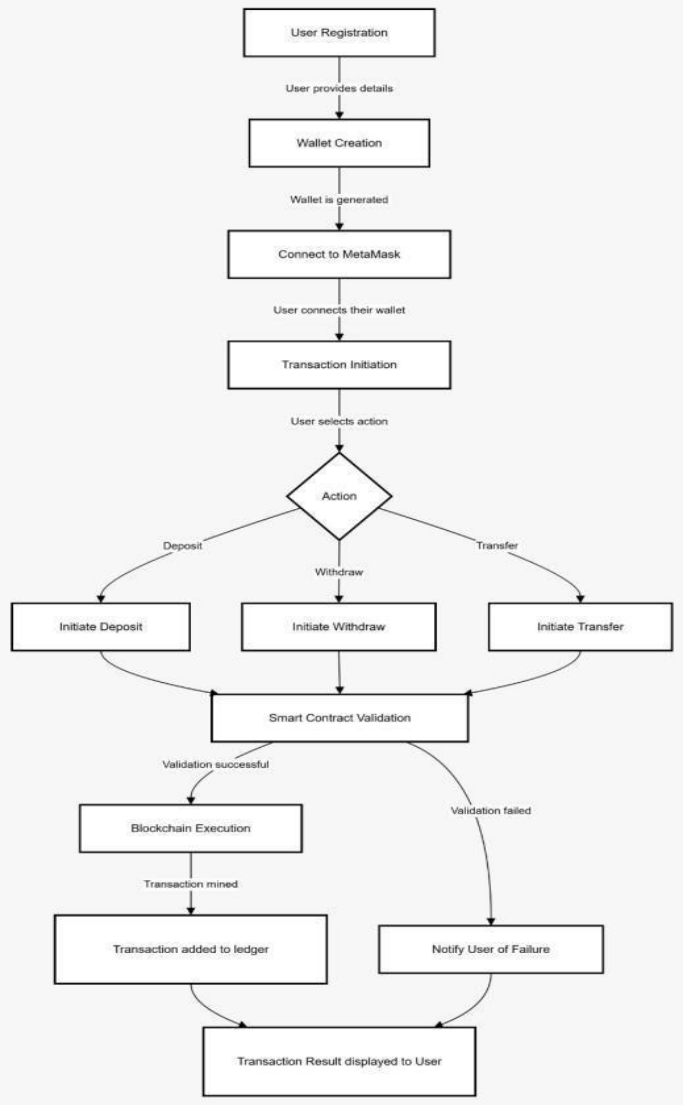

Fig.1.Blockchain Transaction flow

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

IV. IMPLEMENTATION

The implementation of the Secure E-Wallet Using Blockchain involved building a fully functional web application integrated with a blockchain network

A. *TECHNOLOGY STACK*

1. Hardhat

Hardhat is a *comprehensive* development environment for Ethereum smart contracts enabling to compile, deploy, test and debug smart contracts locally before they are published to a live blockchain network. Here Hardhat was utilized to:

- Compile Solidity smart contracts and identify any errors.
- Deploy the contracts on a testnet such as Sepolia.

2. Sepolia Testnet

The Sepolia Testnet is a public Ethereum test network used by developers to test their blockchain applications without spending real cryptocurrency. Key features include:

- Provides free test Ether (ETH) for testing wallet transactions.
- Simulates the Ethereum live net environment locally, allowing developers to validate and interact with smart contracts,conditions that closely mirror the live network, ensuring reliable and consistent behavior upon deployment.

3. Etherscan

Etherscan is an Ethereum blockchain explorer that lets users and developers view, track, and verify transactions, wallet addresses, and smart contracts. In this project:

- Etherscan was used to track test transactions on Sepolia, ensuring transparency and correctness.
- Developers could verify that smart contract deployments and wallet transactions were recorded immutably.
- Provided detailed transaction hashes, timestamps, and block confirmations, which helped during testing and debugging.
- Using Etherscan we can find that every transaction is traceable, transparent, and secure, which is crucial for building a trustworthy e-wallet system.B. Security Implementation.

Security was a priority at every stage of the implementation :

- End-to-End Encryption: TLS/SSL protects data exchanged between frontend, backend, and blockchain nodes.
- SHA-256 Hashing: Each transaction is hashed to guarantee data integrity and protect against tampering.
- Smart Contract Validation: Smart contracts automatically verify transactions and prevent double-spending.
- Private Keys Management: MetaMask signs transactions securely without exposing private keys.

B. Deployment and Testing

- The system was deployed with private Ethereum test network to simulate real transactions without real cryptocurrency.
- Functional testing ensured that wallet creation, fund transfer, and transaction history worked correctly.
- Security testing verified that all transactions were hashed and properly recorded, and that MetaMask handled key management securely.

C. Key Features Implemented

- Wallet Creation: Users can create a new wallet which generates a unique address and associated cryptographic keys.
- Balance Display: Users can view real-time wallet balance fetched directly from the blockchain.
- Fund Transfer: Users can transfer funds to other wallets; smart contracts validate and record each transaction on the blockchain.
- Transaction History: Complete transaction history is displayed in a secure, immutable format.
- Notifications: Users receive instant confirmations of successful or failed transactions.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

V. RESULT & DISCUSSION

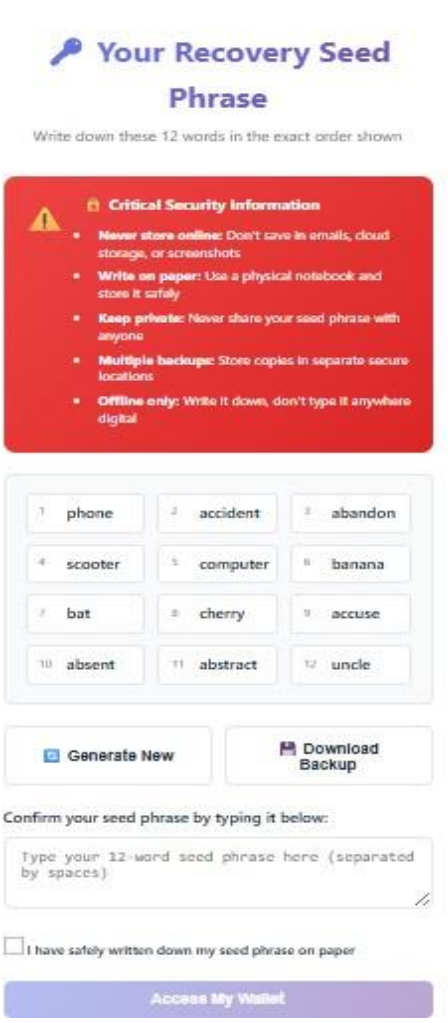

Fig.2.Seed phrase generation

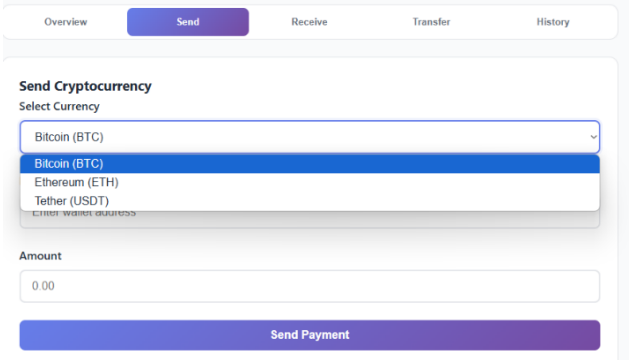

Fig.3.User dashboard

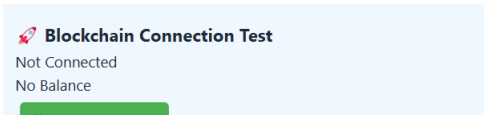

Fig.4. Metamask connection

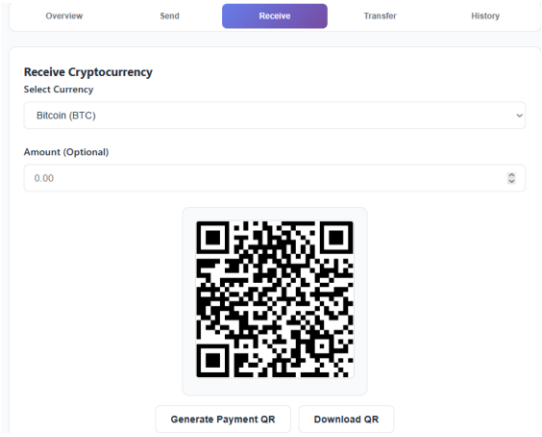

Fig.5. QR code generation

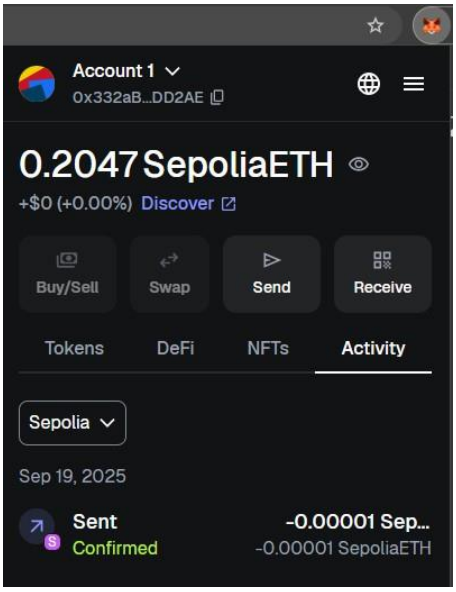

Fig.6.Metamask wallet

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

VII. CONCLUSION

This study demonstrates the practicality of developing a secure and decentralized e-wallet using blockchain technology. By integrating blockchain's fundamental features with security measures such as password authentication, seed phrase recovery, and MetaMask-based transaction signing, the system ensures that users will have ownership over their funds without relying on a centralized authority

Implementation of smart contracts using Ethereum Sepolia testnet facilitated a transparent and verifiable environment for executing transactions. Real-time dashboard monitoring enhanced usability while ensuring that every transfer was recorded permanently on the blockchain ledger. Importantly, private keys were never stored on centralised servers, reinforcing the wallet's non-custodial nature.

This research confirms blockchain's ability to mitigate common weaknesses of traditional wallets, including centralized key storage, phishing, and unauthorized access. It also demonstrates the practical application of academic principles like distributed ledgers, decentralization, and immutability in financial technology.

VIII. FUTURE WORK

While the Secure E-Wallet provides a functional and secure foundation, several enhancements can expand its real-world applicability:

- **Multi-Currency Support**: Extending compatibility to different blockchains so users can manage multiple cryptocurrencies in one wallet.
- **Advanced Security**: Incorporating biometric authentication, and device-level binding for stronger identity protection.
- **Improved Smart Contracts**: Adding features such as recurring payments, multisignature approvals, and gas fee optimisation.
- **Mobile Deployment**: Expanding the system to Android and iOS applications for broader accessibility.
- **Fraud Detection & Monitoring**: Using anomaly detection and transaction alerts to prevent suspicious behavior.
- **Scalability**: Optimising the backend and contracts to handle a higher number of concurrent users and transactions.

- **AI-Powered Risk Analysis**: Machine learning algorithms where used to detect and flag potentially fraudulent transactions before they are finalized.
- **Analytics Dashboard**: Offering users insights into their transaction habits, spending patterns, and wallet usage statistics.
- **Offline Support**: Exploring mechanisms for secure transactions in low-connectivity environments, with later synchronisation to the blockchain.

IX. REFERENCES

[1] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, Oct. 2018, doi: https://doi.org/10.1504/ijwgs.2018.095647.

[2] S. Houy, P. Schmid, and A. Bartel, "Security Aspects of Cryptocurrency Wallets - A Systematic Literature Review," *ACM Computing Surveys*, vol. 56, no. 1, May 2023, doi: https://doi.org/10.1145/3596906.

[3] Yu, Y., Sharma, T., Das, S., and Wang, Y., 2024, May. "Don't put all your eggs in one basket": How Cryptocurrency Users Choose and Secure Their Wallets. In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems(pp 1-17)

[4] Nakamoto, S., 2008. Available at SSRN 3440802.

[5] Jokić, S., Cvetković, A.S., Adamović, S., Ristić, N. and Spalević, P., 2019. Comparative analysis of cryptocurrency wallets vs traditional wallets. Economika,65(3).

[6] Adhav, P., Wagh, S.B., Kinikar, R.C., Shinde, S.S., and Panchal R.M.,2021.INTERNATIONAL JOURNAL(12)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

[7] Nowroozi, E., Seyedshoari, S., Mekdad, Y., Savaş, E. and Conti, M., 2022. Cryptocurrency wallets: assessment and security. In Blockchain for Cybersecurity in Cyber-Physical Systems(pp 1-19). Cham: Springer International Publishing.

[8] Sable, N.P., Rathod, V.U., Sable, R., and Shinde, G.R., 2022, December. The secure e-wallet is powered by blockchain and distributed ledger technology.

[9] Guo, H. and Yu, X., 2022. A survey on blockchain technology and its security. Blockchain research and applications,3(2), p.100067.

[10] Bui-Huu, D., Le-Nhat, T., and Nguyen-An, K., 2024, December. Blockchain-Powered e-Wallet: Enhancing Security and Fraud Detection in Online Payments. In 2024, 1st International Conference On Cryptography and Information Security (VCRIS)(pp 1-6). IEEE.

[11] Yadav, N.S., Goar, V. and Kuri, M., 2020. Crypto Wallet: a perfect combination of blockchain and a security solution for banking. International Journal of Psychosocial Rehabilitation 24 (2),pp.6056-6066.

[12] Mitawa, A., 2024. Enhancing Financial Transaction Security With Blockchain Technology. Educ.Administration Theory Pract. J., no.

[13] Le, T.V. and Hsu, C.L., 2021.The literature review of blockchain technology: Security properties, applications, and challenges.Journal of Internet Technology,22(4), pp.789-802.

[14] Goyal, A., 2023, May. Blockchain Wallet for Secure Transactions. In Proceedings of the KILBY 1007th International Conference on Computing Sciences.

[15] Roy, S., 2025. Wallet Management Practices in Cryptocurrency Exchanges: Security, Compliance, and Future Innovations. Compliance and Future Innovations (January 25, 2025).

[16] Erinle, Y., Kethepalli, Y., Feng, Y. and Xu, J., 2025. Sok: Design,vulnerabilities and security measures of cryptocurrency wallets. Computer Networks, p.111691.

[17] Sarwan, K., Thore, S., Satav, N., Kamble, P., and Mandal, D., 2021. A secure e-wallet system using blockchain.