VISVESWARAYA TECHNOLOGICAL UNIVERSITY

"Jnana Sangama", Belgaum-590014, Karnataka

SYNOPSIS ON
SECURE E – WALLET USING BLOCKCHAIN

Submitted in partial fulfillment for the requirement of 6th semester

BACHELOR OF ENGINEERING

IN

CSE – CYBER SECURITY

Submitted By

GUNAVATHI C [1AH22CY016]
HARSHITHA N [1AH22CY019]
VEENA AH [1AH22CY060]

Under the Guidance of

Mrs. K.P SANGEETHA

Assistant Professor

DEPARTMENT OF CSE-CYBER SECURITY

DEPARTMENT OF CSE – CYBER SECURITY

ACS COLLEGE OF ENGINEERING

#74, Kambipura, Mysore Road, Bengaluru 560074

(An ISO 9001:2015 Certified Institute)

2024-2025

ACS COLLEGE OF ENGINEERING

#74, Kambipura, Mysore road, Bengaluru – 560074

(An ISO 9001:2015 Certified Institute)

Department of CSE – CYBER SECURITY

CERTIFICATE

This is to certify that the Project Work entitled **" Secure E-Wallet Using Blockchain"** has been successfully submitted by **GUNAVATHI C (1AH22CY016), HARSHITHA N (1AH22CY019) , VEENA AH (1AH22CY060) ,** Bonafide students at **ACS COLLEGE OF ENGINEERING** affiliated to **Visvesvaraya Technological University, Belgaum** during the year 2025-2026. It is certified that all corrections/ suggestions indicated for the Internal Assessment have been incorporated in the report submitted to the department. The Project report has been approved as it satisfies academic requirements with respect to Academic work as prescribed in the 7th semester.

Signature of the Guide	**Signature of the Coordinator**	**Signature of the HOD**
Mrs.K.P.Sangeetha Assistant Professor, CSE-CYBERSECURITY ACSCE, Bangalore	**Dr.M.Karuppasamy** Assistant Professor, CSE-CYBER SECURITY ACSCE, Bangalore	**Dr.M.Karuppasamy** Professor & HOD, CSE-CYBER SECURITY ACSCE, Bangalore

ACKNOWLEDGMENT

We take this opportunity to express our sincere gratitude and respect to the **ACS College of Engineering,** Bengaluru for providing me an opportunity to carry out our Project report.

We express deep regards to our honorable chairman **Dr. A.C. Shanmugam** for providing mean opportunity to fulfil my ambition in this prestige institute.

We would like to express our immense gratitude to **Dr. Anandthirtha B Gudi,** Principal, ACS College of Engineering, Bengaluru, for his timely help and inspiration during the tenure of the course.

We express sincere regards and thanks to **Dr. M. Karuppasamy,** Professor & HOD, Dept of CSE - Cyber Security, ACSCE, Bengaluru for the encouragement and support throughout the work.

We are highly thankful to our guide **Mrs .K. P. Sangeetha ,** Assistant Professor, Dept of CSE-Cyber Security , ACSCE for giving a valuable suggestion, providing cooperation and moral support towards completion of the Project Work.

CONTENTS

ABSTRACT

A crypto wallet is a digital wallet that allows users to securely store, manage, and transfer their cryptocurrencies. It is a perfect combination with blockchain technology and provides a secure solution for banking. Blockchain technology is the backbone of the cryptocurrency industry, and it ensures the security and immutability of transactions. Cryptocurrency wallets leverage blockchain technology to ensure that transactions are secure, transparent, and tamper-proof. Crypto wallets come in different forms, including hardware wallets, software wallets, and mobile wallets. Each type of wallet has its unique features, advantages, and disadvantages. For example, hardware wallets offer the highest level of security as they store private keys offline, while mobile wallets offer convenience and accessibility. Cryptocurrency wallets are also a perfect solution for banking because they offer users more control over their funds. Crypto wallets can offer enhanced security features, such as two-factor authentication, multi-signature support, and biometric authentication. These features help to ensure that users' funds are secure and protected from unauthorised access.

Key words: Bank, Finance, PI, Cryptocurrency, Blockchain, Crypto wallet, E-wallet.

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. Blockchain works like a shared digital ledger which 2 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.

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.
- Phishing attacks: Fraudulent emails or sites trick users into revealing credentials.
- Weak authentication: Simple password or OTP systems are often compromised.
- Centralized data: Single points of failure lead to large-scale breaches.
- Limited transparency: Users find it hard to track or audit their own transactions.

LITERATURE SURVEY

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 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- 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.

OBJECTIVE OF THE PROPOSED PROJECT

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 :

- To develop a decentralized wallet architecture with the help of blockchain for secure transactions.
- To employ cryptographic mechanisms to maintain data privacy and be free from unauthorized access.
- To integrate wallet security through a combination of hot and cold wallet features.
- To eliminate central authority dependency and establish user-controlled authentication.
- 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.

METHODOLOGY FOLLOWED

A. System Architecture

1. 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. Algorithms 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.

1. Requirement Analysis

- Identify user interactions in the wallet
- Identify blockchain components
- Define authentication and transaction flow

2. System Architecture Design

The proposed architecture includes:

- User Interface
- Authentication Module
- Blockchain Network (Ethereum Testnet / Private Chain)
- Smart Contracts
- Wallet Management System
- Transaction Validator
- Secure Key Storage Module

3. Blockchain Setup

- Using Ethereum blockchain (Sepolia testnet or private network)
- Writing smart contracts in Solidity
- Deploying using Remix IDE / Hardhat

4. Smart Contract Implementation

Smart contracts handle:

- Wallet creation
- Balance check
- Transaction initiation
- Transfer verification
- Recording transaction logs

5. Frontend + Backend Development

- Frontend: HTML, CSS, JavaScript
- Backend: Node.js or Express.js
- Blockchain Interaction: Web3.js or Ethers.js

6. Security Enhancements

- Multi-factor authentication (OTP + password + key pair)
- SHA-256 hashing
- AES encryption of sensitive data
- Secure API communication
- Prevention of replay attacks using timestamps

7. Testing

- Module testing
- Integration testing
- Smart contract testing
- Security penetration testing

8. Deployment and Evaluation

Deploy the final system on the blockchain test network and evaluate performance, gas usage, security, and real-world usability.

OUTCOME OF PROPOSED PROJECT

- A decentralized e-wallet system powered by blockchain.
- Improved safety, transparency, and trust in financial transactions.
- Tamper-proof and immutable transaction logs.
- Reduced fraud and unauthorized access.
- Elimination of intermediaries using smart contracts.
- Real-time verification of transactions.
- Strong user authentication system.

The project results in a highly secure and efficient e-wallet architecture suitable for modern digital financial systems.

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 3 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 decentralization, like distributed ledgers, and immutability in financial technology.

Blockchain technology significantly enhances the security of e-wallet systems by introducing decentralization, transparency, and immutability. By using smart contracts, cryptographic algorithms, and distributed ledger technology, the proposed e-wallet system ensures safe and trustworthy transactions.

The architecture eliminates many weaknesses of traditional centralized wallets and provides users with a secure environment for digital payments. The project demonstrates blockchain’s potential to transform the fintech industry and provides a foundation for secure, scalable, and user-friendly e-wallet solutions in the future.

REFERENCES

[1] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: survey,” International Journal of Web and Grid Services, a 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 https://doi.org/10.1145/3596906. 2023, doi:

[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. AvailableatSSRN3440802.

[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)

[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.andKuri,M.,2020.CryptoWallet: aperfectcombination ofblockchainandasecurity solutionfor 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.JournalofInternetTechnology,22(4),pp.789-802.

[14] Goyal, A., 2023, May. Blockchain Wallet for Secure Transactions.InProceedingsoftheKILBY1007th International Conference on Computing Sciences.

[15] Roy, S., 2025. Wallet Management Practices in CryptocurrencyExchanges: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.ComputerNetworks,p.111691.

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