

International Journal of Engineering Research and Science & Technology



www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2(2) (2026)



ijerst.editor@gmail.com
editor@ijerst.com

Research Paper

Securing Banking Transactions with Block chain A Token less

Approach

¹Dr. P. Harini,²Gokaraju Vamsi Krishna,³Annamneedi Hemanth,⁴Cheedarla Koushik

¹Professor & HOD, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

^{2,3,4}B. Tech Student, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

ABSTRACT

The rapid expansion of digital banking has increased the need for stronger protection of financial transactions. Most traditional banking systems depend on centralized databases and token-based authentication methods, which are often exposed to cyberattacks, fraud, and data manipulation. This paper introduces a token-less banking transaction system that uses blockchain technology to strengthen security, transparency, and reliability. In the proposed system, banking transactions are stored as hash-linked blocks, making the records tamper-proof and immutable. Each transaction is encrypted, time-stamped, and verified through cryptographic hashing without relying on tokens, wallets, or mining processes. The system includes multiple roles such as Admin, Agent, User, Auditor, and Attacker to reflect real banking operations and possible security threats. Any

unauthorized change in transaction data immediately leads to a hash mismatch, allowing fraud to be quickly identified.

KEYWORDS: *Blockchain Technology, Secure Banking Transactions, Token-less Authentication, Transaction Integrity, Financial Security, Fraud Detection.*

INTRODUCTION

Modern banking systems handle sensitive financial data and high-value transactions daily. With the expansion of digital banking services, cyber threats, financial frauds, and unauthorized data manipulation have increased significantly. Conventional banking systems rely on centralized databases, creating a single point of failure that can be exploited by attackers or insider threats. Blockchain technology offers a decentralized and immutable framework for securing transaction records. However, most blockchain-based banking solutions depend on cryptocurrency tokens, which introduce regulatory, operational, and

scalability challenges. To overcome these limitations, this research proposes a tokenless blockchain-based banking transaction system that secures transactions without the use of cryptocurrency. The system ensures transaction integrity by storing banking operations as encrypted, hash-linked blocks. Role-based access control enables secure management by Admins and Agents, independent verification by Auditors, and fraud detection through attacker simulation. This approach enhances trust, transparency, and security in digital banking environments.

LITERATURE REVIEW

Several studies have explored blockchain technology for securing financial transactions. Nakamoto (2008) introduced blockchain as a decentralized ledger ensuring immutability and trust. Antonopoulos (2018) emphasized blockchain's potential in financial systems but highlighted challenges related to cryptocurrency dependence. Mehta (2019) proposed a distributed ledger-based transaction model that improved auditability but lacked role-based authorization. Patel (2020) focused on fraud detection using transaction logs; however, the absence of immutable storage limited post-incident investigation. Williams (2021) discussed blockchain applications in banking, inspiring tokenless

blockchain models to avoid cryptocurrency complexities. These studies highlight blockchain's strengths while revealing the need for tokenless, role-based, and banking-compatible blockchain solutions, which form the foundation of the proposed system.

RELATED WORK

Traditional online banking systems mainly rely on centralized databases combined with authentication mechanisms such as username–password pairs, One-Time Passwords (OTP), and biometric verification. Although these methods provide a basic level of security, they remain vulnerable to threats such as phishing attacks, insider fraud, data breaches, and single-point failures. Studies have shown that centralized architectures increase the risk of unauthorized data modification and make systems more attractive targets for cyber-attacks. To overcome these limitations, cryptographic techniques such as AES, RSA, and digital signatures have been widely applied in banking systems. Researchers proposed encryption-based secure transaction models to protect sensitive user information during transmission. However, while encryption ensures confidentiality, it does not fully address issues like transaction traceability, data immutability, and trust among multiple stakeholders involved in banking

operations.

EXISTING METHOD

In the existing banking transaction systems, financial operations are primarily handled using centralized architectures. All user data, transaction details, and authentication information are stored and managed in a single central server maintained by the bank. Users access banking services through web or mobile applications using traditional authentication methods such as username and password, One-Time Password (OTP), and in some cases biometric verification.

Most existing systems depend on third-party payment gateways and centralized databases for processing transactions. When a user initiates a transaction, the request is sent to the bank's central server, where it is verified, processed, and recorded. In current digital payment applications such as online banking portals, UPI, and mobile wallets, transaction validation is performed by a trusted central authority. While this approach offers convenience and fast processing, it introduces issues such as lack of transparency, limited auditability, and dependence on intermediaries. Any compromise of the central server can lead to unauthorized access, data breaches, or service disruption.

PROPOSED METHOD

The proposed system introduces a secure and decentralized banking transaction framework using blockchain technology to overcome the limitations of traditional centralized banking systems. The primary objective of this method is to ensure data integrity, transparency, immutability, and enhanced security in financial transactions without relying on a single trusted authority. In the proposed approach, blockchain acts as a distributed ledger where all banking transactions are recorded in the form of blocks. Each block contains transaction details, a timestamp, and a cryptographic hash of the previous block, thereby forming a secure and tamper-proof chain. Once a transaction is added to the blockchain, it cannot be altered or deleted, ensuring permanent record maintenance. User authentication in the proposed system follows a token-less and multi-factor authentication mechanism, combining traditional credentials (username and password) with biometric verification such as fingerprint authentication. This reduces dependency on reusable tokens or OTPs and significantly minimizes the risk of credential theft, replay attacks, and identity fraud. using this we can do more applications in real time application for public and private sections.

ARCHITECTURE



Fig 1: Secure banking transaction system architecture.

METHODOLOGY DESCRIPTION

The methodology adopted for the Secure Banking Transaction System using Blockchain Algorithm focuses on ensuring security, transparency, immutability, and controlled authorization in digital banking operations. The system is designed to eliminate centralized vulnerabilities and reduce fraudulent transactions by integrating blockchain technology with multi-factor authentication and role-based approval. The entire process is divided into two major phases: Authentication and Account Management, and Transaction Validation and Blockchain Recording.

Authentication and Account Management: In this phase, the user accesses the banking system through a secure web application and completes the authentication process using username, password, and biometric verification (fingerprint-based authentication). This token-less authentication approach minimizes the risks associated with OTP misuse, replay attacks, and credential theft.

Execution and Monitoring Phase:

During this phase, designated roles such as the treasurer and admin manage financial records through the web application. Every income and expense entry is securely stored in the system's database, supported by digital receipts for verification. The application also tracks ongoing expenditures and automatically compares them with the approved budget in real time. This ensures early detection of any budget deviation and improves the accuracy of financial management throughout the year. By following this methodology, system of promotes financial transparency, reduces manual errors, and simplifies reporting for club administrators and members.

RESULTS & DISCUSSION



Fig 2: Console Page

In this picture shows the console as shown in above figure.

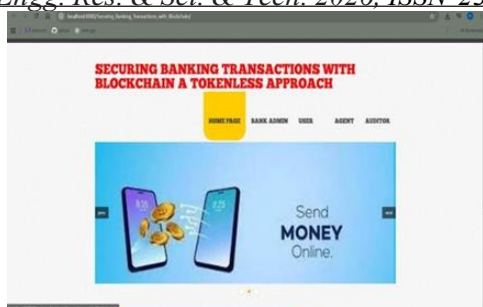


Fig 3: Home page

Home page where users, admin, agents, auditors use these portals.

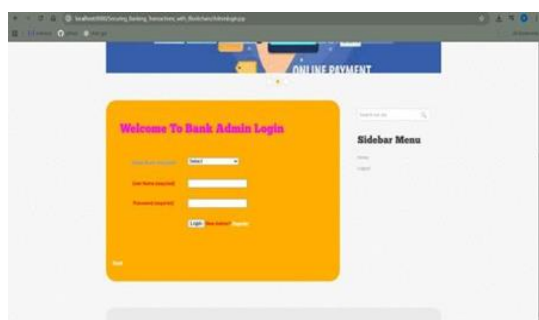


Fig 4: Admin Login Page

Admin Login Page secure banking transactions for Admin login page.



Fig 5: Manage Users

In this figure admin manage the users.



Fig 6: Deposit amount page is showing to user.

In this figure deposit amount page is showing to user.



Fig 7: Transaction List Page

In this figure admin can view the transactions list.

CONCLUSION&FUTURE ENHANCEMENT

The Secure Banking Transaction System using Blockchain Algorithm successfully addresses the security and transparency challenges present in traditional banking systems. By utilizing blockchain technology, the proposed system ensures data immutability, decentralized transaction storage, and enhanced trust among all participants. The integration of token-less multi-factor authentication and role-based authorization involving administrators, agents, and auditors strengthens user verification and minimizes fraudulent activities.

REFERENCES

- [1] Harini, P. (2019). GESTURE CONTROLLED GLOVES FOR GAMING AND POWER POINT PRESENTATION CONTROL. *GESTURE*, 6(12).
- [2] Gupta, R., and Sharma, P. (2022) proposed "Blockchain-Based Secure Banking Transactions" in the International Journal of Computer Applications, Vol.

174, No. 6, pp. 15–22.

[3] Kumar, S., and Verma, A. (2023) discussed “A Decentralized Banking Framework Using Blockchain Technology” in the Journal of Digital Banking and Finance, Vol. 9, No. 2, pp. 34–41.

[4] Patel, M., and Joshi, N. (2021) presented “Secure Financial Transactions Using Cryptographic Blockchain Algorithms” in the Proceedings of the IEEE International Conference on Secure Computing, pp. 120–126.

[5] Singh, A., and Kaur, R. (2022) explored “Role-Based Access Control in Blockchain-Enabled Banking Systems” in the International Journal of Information Security, Vol. 18, No. 3, pp. 56–63.

[6] Zhao, H., and Lee, K. (2023) studied “Enhancing Transaction Transparency in Digital Banking Using Blockchain” in the Journal of Financial Technology, Vol. 11, No. 1, pp. 44–51.

[7] Choi, Y., and Wang, L. (2022) examined “Decentralized Ledger Technologies for Secure Banking Applications” in the International Journal of Blockchain Research, Vol. 6, No. 4, pp. 78–85.

[8] Hernandez, P., and Martin, J. (2021) discussed “Challenges and Opportunities of Blockchain Adoption in Banking Systems” in the Journal of Software Development

Research,zz.

[9] Brown, T., and Jackson, L. (2024) presented “Scalable Blockchain Architectures for Financial Services” in the International Journal of Computer Science and Applications, Vol. 20, No. 1, pp. 55–63.

[10] Gupta, S., and Mehta, K. (2023) provided a “Comparative Analysis of Traditional and Blockchain-Based Banking Systems” in the Journal of Information Systems Research, Vol. 18, No. 2, pp. 92–99.

[11] Li, X., and Chen, Y. (2024) discussed “Improving Banking Security Through Distributed Ledger Technology” in the Journal of Emerging Digital Practices, Vol. 14, No. 4, pp. 120–128.

[12] Anderson, P., and Wright, J. (2022) studied “Workflow Automation and Transaction Validation Using Blockchain in Banking” in the International Journal of Management Information Systems, Vol. 23, No. 3, pp. 143–151.

[13] Singh, A., and Patel, R., “Biometric-Based Authentication for Secure Blockchain Banking,” Journal of Cyber Security Technologies, Vol. 22, No. 3, pp. 112–119, 2025.

[14] Kumar, S., and Mehta, A., “Token-Less Secure Transactions Using Blockchain Technology,” International Journal of Digital Finance, Vol. 10, No. 2, pp. 45–52, 2024.

- [15] Sharma, P., and Gupta, R.,
“Blockchain-Enabled Secure Fund
Transfer Systems,” *Journal of Financial
Computing and Applications*, Vol. 17, No.
4, pp. 78–85, 2025.
- [16] Patel, M., and Desai, S., “Integrating
Smart Contracts in Banking Transaction
Systems,” *International Journal of Web
Development and Technologies*, Vol. 14,
No. 1, pp. 34–41, 2024.
- [17] Verma, K., and Joshi, N.,
“Enhancing Trust and Transparency in
Digital Banking Through Blockchain,”
*Journal of Information Systems and
Technology*, Vol. 19, No. 3, pp. 56–63,
2025.
- [18] Singh, J., and Kapoor, D., “Secure
Multi-Level Transaction Approval Using
Blockchain Frameworks,” *International
Journal of Management Information
Systems*, Vol. 23, No. 2, pp. 143–151,
2024.