Block Chain Technology for Secure Transaction

Dr.D.Deepika[1], Ms. B. Varalaxmi[2],
Golipally Greeshma Reddy[3], Paka Niharika[4]
[1,2]Assistant Professors, Department of Emerging Technologies, Mahatma Gandhi Institute of Technology, Hyderabad, Telangana – 500 075
[3,4]Students, Department of Emerging Technologies (CSE-AI&ML), Mahatma Gandhi Institute of Technology, Hyderabad, Telangana – 500 075
ddeepika_cse@mgit.ac.in

How to Cite this Article:

Varalaxmi, B., Reddy, G. G. & Niharika, P. (2026). Block Chain Technology for Secure Transaction. International Journal of Creative and Open Research in Engineering and Management, 02. https://doi.org/10.55041/ijcope.v2i6.227

https://doi.org/10.55041/ijcope.v2i6.227

ABSTRACT

The rapid growth of digital banking has improved convenience and accessibility but has also introduced significant security challenges, including phishing attacks, data breaches, OTP interception, and unauthorized transactions. Traditional banking systems rely heavily on centralized databases and token-based authentication mechanisms, which remain vulnerable to various cyber threats. This paper proposes a tokenless blockchain-based secure transaction framework that employs digital signatures and a permissioned blockchain ledger for authentication and transaction validation. The proposed system eliminates dependency on OTPs and external communication networks while ensuring transparency, immutability, and tamper-resistant transaction records. SHA-256 hashing is used to secure transaction blocks, and only authorized banking nodes participate in the validation process. Experimental implementation demonstrates improved security, enhanced auditability, and greater reliability compared to conventional banking systems.

Keywords: Blockchain, Digital Banking, Tokenless Authentication, SHA-256, Digital Signatures, Secure Transactions.

1. INTRODUCTION

Digital banking has transformed financial services by enabling fast and convenient transactions. However, increasing dependence on centralized infrastructures and token-based authentication methods such as OTPs and SMS verification has exposed banking systems to cyberattacks including phishing, SIM-swapping, and credential theft. Blockchain technology offers a decentralized approach to transaction validation and data storage, providing enhanced security and transparency.

This research proposes a tokenless blockchain-based banking system that utilizes cryptographic digital signatures and a permissioned blockchain network. The proposed framework aims to reduce vulnerabilities associated with traditional authentication mechanisms while maintaining secure and transparent transaction processing.

2. LITERATURE REVIEW

Recent studies have explored blockchain applications in authentication and financial security. Zhang et al. introduced decentralized identity systems for tokenless authentication, while Ali et al. proposed blockchain-backed authentication using cryptographic signatures. Li et al. developed blockchain-based identity verification frameworks for banking applications. Other researchers have highlighted the benefits of smart contracts, decentralized governance, and immutable ledgers in enhancing transaction security and reducing fraud.

Despite these advancements, challenges such as scalability, interoperability, and efficient key management remain important research concerns.

3. PROPOSED METHODOLOGY

The proposed system replaces token-based authentication with cryptographic digital signatures and a permissioned blockchain ledger. Users authenticate transactions using private-public key cryptography rather than OTPs or hardware tokens.

The transaction workflow includes:

1. User authentication through digital signatures.
2. Transaction verification by authorized banking nodes.
3. SHA-256 hash generation for transaction integrity.
4. Block creation and validation.
5. Storage of validated transactions in an immutable blockchain ledger.

The decentralized architecture eliminates single points of failure and provides enhanced resistance against unauthorized modifications.

4. SYSTEM ARCHITECTURE

The system follows a three-layer architecture:

Presentation Layer

Provides JSP-based interfaces for users, administrators, auditors, and agents.

Application Layer

Contains transaction processing, authentication modules, blockchain management, smart contract execution, and auditing mechanisms.

Data Layer

Stores user information in MySQL databases and transaction records within a permissioned blockchain ledger.

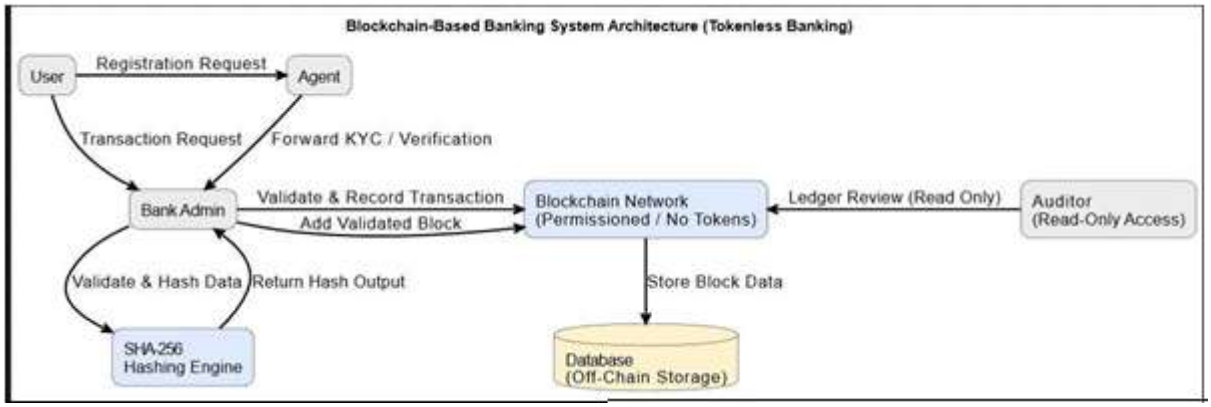

Figure 1: System Design Architecture

The architecture ensures secure transaction validation, transparency, and scalability.

5. RESULTS AND DISCUSSION

A prototype banking application named BlockSecure Bank was developed using Java/J2EE and MySQL. The system supports user registration, account authorization, transaction processing, auditing, and blockchain ledger management.

The blockchain ledger records every approved transaction with associated hash values and previous block references, ensuring data integrity and tamper resistance. Multi-level authorization involving users, auditors, agents, and administrators strengthens security and accountability.

Figure 2 : Home Page of BlockSecure Bank

The implementation demonstrates:

- Elimination of OTP-related vulnerabilities.
- Improved transaction transparency.
- Enhanced resistance to data tampering.
- Secure audit trail generation.

- Reliable decentralized transaction validation.

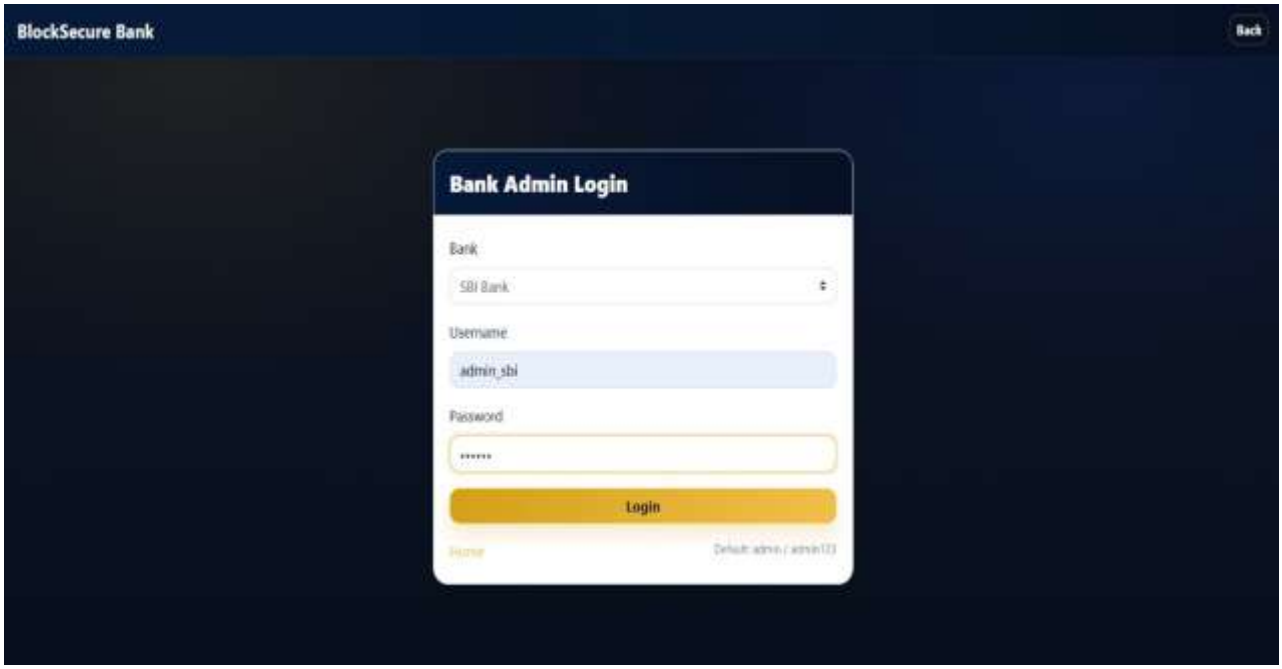

Figure 3 : Bank Admin Login Interface

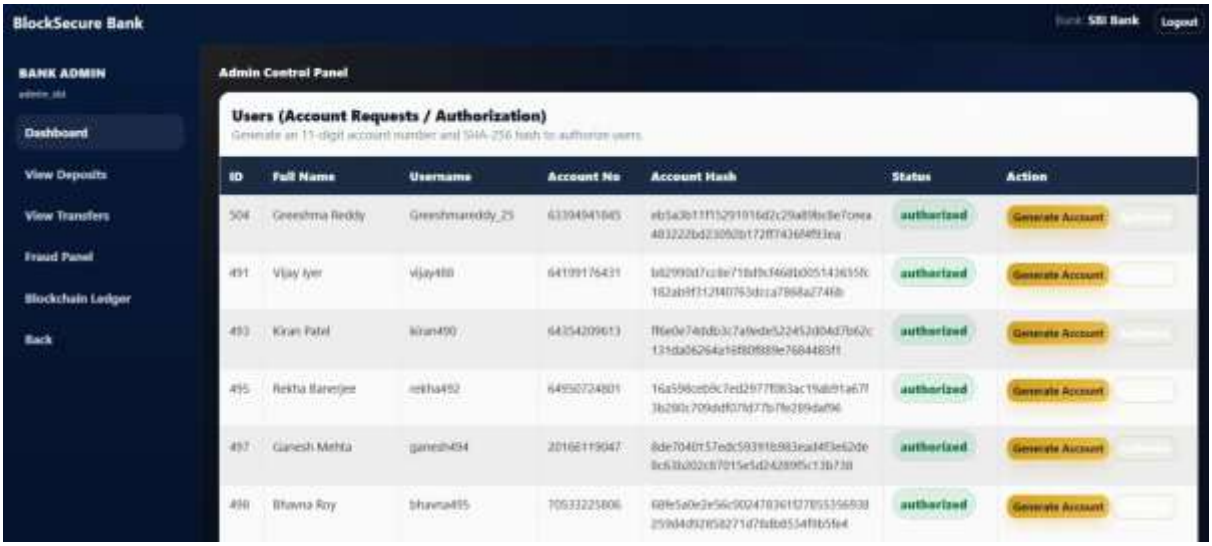

Figure 4: Admin Dashboard – User Authorization Panel

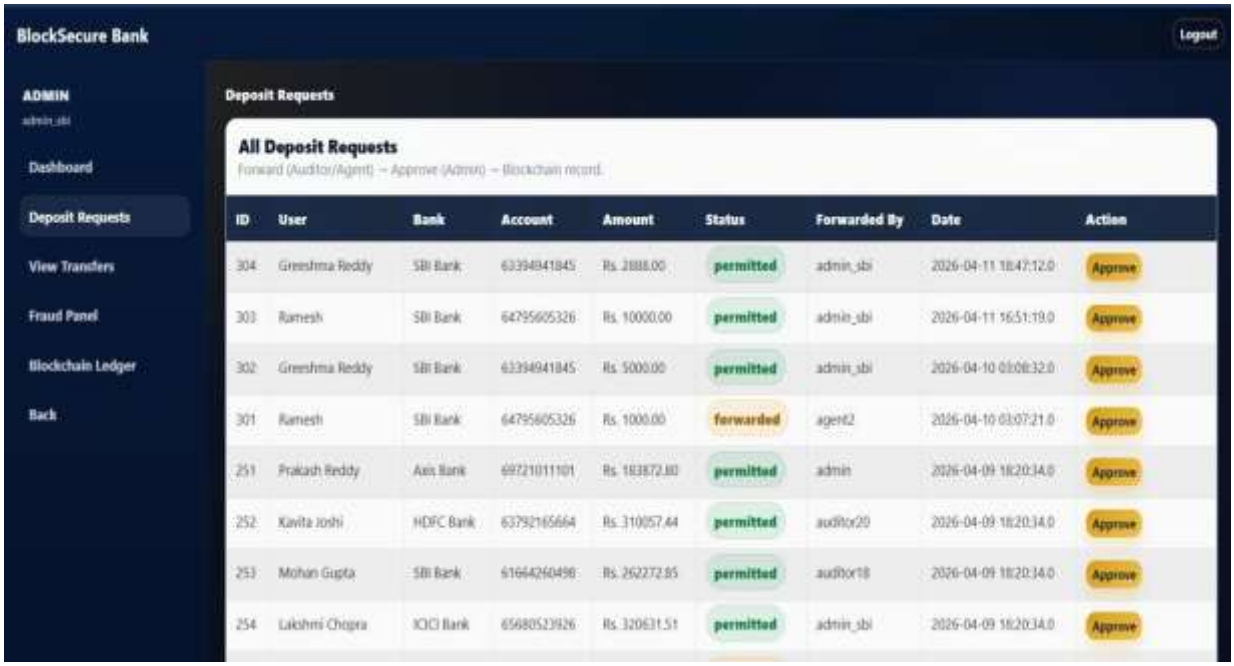

Figure 5 : Admin Deposit Requests Panel

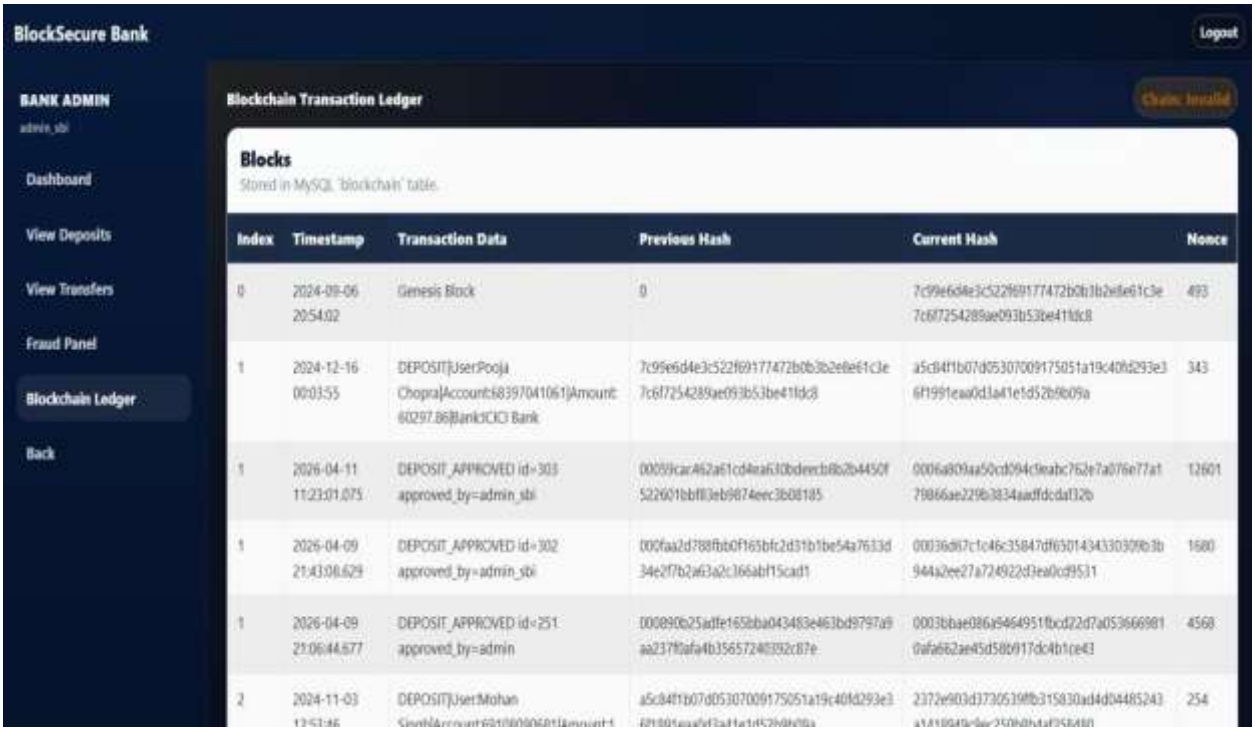

Figure 6 : Blockchain Transaction Ledger View

Figure 7 : New User Registration Interface

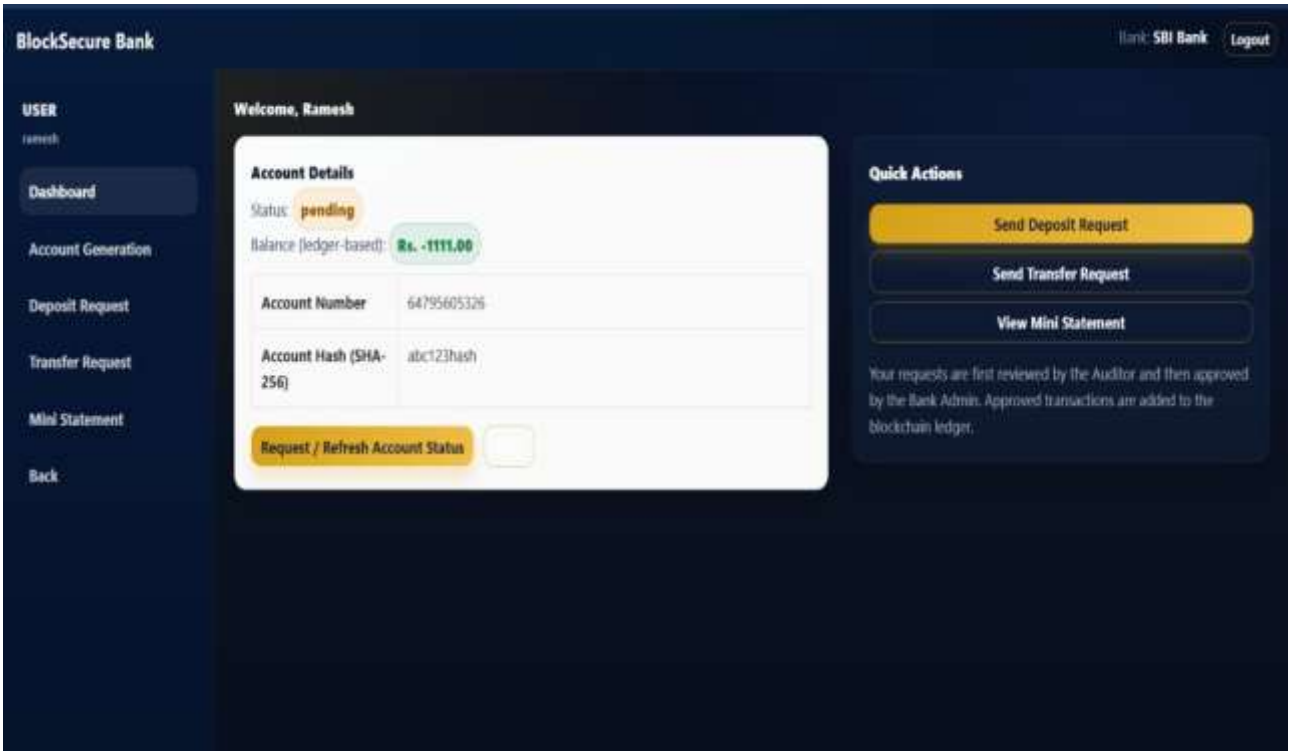

Figure 8 : User Dashboard Overview

6. CONCLUSION AND FUTURE WORK

This paper presented a tokenless blockchain-based secure banking framework designed to overcome limitations of traditional token-dependent authentication systems. By leveraging digital signatures, SHA-256 hashing, and permissioned blockchain technology, the system provides secure, transparent, and tamper-proof transaction processing.

Future work includes integration with Hyperledger Fabric or Ethereum, deployment on cloud platforms, incorporation of smart contracts for automated verification, implementation of AI-based fraud detection, and development of mobile banking applications.

REFERENCES

[1] Y. Zhang et al., “Decentralized Identity (DID) Systems for Secure Identity Management,” IEEE Access, vol. 8, pp. 12345–12355, 2020.
[2] M. Ali et al., “Blockchain-Based Authentication Mechanisms Beyond OTP Systems,” Future Generation Computer Systems, vol. 102, pp. 500–510, 2019.
[3] X. Li et al., “A Blockchain-Based Digital Identity Authentication Framework for Banking Systems,” Computer Networks, vol. 150, pp. 100–110, 2018.
[4] V. Golosova and A. Romanovs, “Blockchain Architecture for Secure Banking Transactions Using Smart Contracts,” Procedia Computer Science, vol. 104, pp. 45–50, 2018.
[5] M. Atzori, “Blockchain Technology and Decentralized Governance: Is the State Still Necessary?” Journal of Governance and Regulation, vol. 6, no. 1, pp. 45–62, 2017.
[6] P. Treleaven, R. G. Brown, and D. Yang, “Blockchain Technology in Financial Services,” Journal of Financial Perspectives, vol. 3, no. 3, pp. 1–17, 2017.
[7] D. L. K. Chuen and R. Deng, “Blockchain Applications in Financial Services and Banking,” Journal of Financial Services Research, vol. 52, pp. 75–98, 2017.
[8] N. Kshetri, “Can Blockchain Strengthen the Internet of Things?” IT Professional, vol. 19, no. 4, pp. 68–72, 2017.
[9] J. Yli-Huumo et al., “Where Is Current Research on Blockchain Technology?—A Systematic Review,” PLOS ONE, vol. 11, no. 10, pp. 1–27, 2016.
[10] C. Catalini and J. S. Gans, “Some Simple Economics of the Blockchain,” MIT Sloan Research Paper, pp. 1–28, 2016.
[11] N. A. Popova and N. G. Butakova, “Improving Security and Performance in Banking Information Systems,” Procedia Computer Science, vol. 66, pp. 234–241, 2015.
[12] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[13] G. Peters and E. Panayi, “Understanding Distributed Ledger Technology and Blockchain in Finance,” Journal of Banking and Financial Technology, vol. 1, no. 2, pp. 1–15, 2015.
[14] V. Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform,” Ethereum White Paper, 2015.