Blockchain-Driven Security Enhancements in Modern Banking System

Authors

1st Tejas K B Dept. of CSE,
Don Bosco Institute of Technology Bengaluru, India, tejaskb2004@gmail.com

2nd Vedangh G Dept. of CSE,
Don Bosco Institute of Technology Bengaluru, India, vedanghg@gmail.com

3rd Suhas P L Dept. of CSE,
Don Bosco Institute of Technology Bengaluru, India, suhaspl1817@gmail.com

4th Yadunandan B A Dept. of CSE,
Don Bosco Institute of Technology Bengaluru, India, yadunandanstudies@gmail.com

Corresponding Author (Guide)
Mohammed Kaleem Assistant Professor Dept. of CSE,
Don Bosco Institute of Technology
mkaleem@dbit.co.in

Abstract

Traditional banking systems often struggle with high transaction fees, slow processing times, and se- curity vulnerabilities due to their centralized nature. These issues not only inconvenience users but also expose financial data to risks like fraud and breaches. To address these challenges, this project introduces a blockchain-powered digital wallet specifically designed for banking. By leveraging de- centralization, the system improves transparency, accelerates transactions, and strengthens security. Key security enhancements include bcrypt for secure password storage and AES-GCM encryption to safeguard sensitive data. Additionally, two-factor authentication via mobile apps provides an extra layer of protection for user accounts. A notable improvement is the transition from SHA-256 to the more advanced SHA-512 hashing method, which offers stronger resistance to brute-force attacks. De- signed for security, ease of use, and future adaptability, this digital wallet presents a trustworthy and modern alternative to both traditional banking systems and existing blockchain solutions.

Keywords

Blockchain, Decentralization, Cryptography, Banking, Security, Wallet system

Introduction

The current banking system relies on centralized institutions to process transactions, manage accounts, and secure funds. While this structure has long provided regulation and trust, it also comes with sig- nificant inefficiencies. High operational costs, slow settlement times—especially for international transactions—and limited transparency create ongoing frustrations. Additionally, the reliance on a single point of control leaves traditional banking systems susceptible to cyberattacks, fraud, and un- expected service disruptions.

Blockchain technology offers a promising alternative by decentralizing financial transactions through a distributed ledger system. With cryptographic security and consensus mechanisms, blockchain en- sures transparency, data

integrity, and protection against unauthorized alterations—all without the need for a central authority. This results in faster, more cost-effective, and highly secure transactions, making blockchain a powerful tool for the future of financial services.

However, many existing blockchain wallets struggle with security, scalability, and adaptability. Some still use outdated cryptographic methods, offer minimal authentication measures, and lack the resili- ence needed to withstand emerging cybersecurity threats, such as quantum computing risks. These shortcomings have limited their adoption in heavily regulated financial sectors.

This project aims to bridge that gap by developing a blockchain-powered wallet specifically designed for banking applications. By incorporating advanced cryptographic techniques, two-factor authentica- tion, fraud detection, and preparations for post-quantum security, the system delivers a secure and scalable digital financial solution. With a focus on long-term adaptability, this initiative aligns with the global shift toward decentralized banking while providing users with a reliable, future-ready plat- form.

Literature Review

Several studies have explored blockchain technology in financial systems, emphasizing its role in enhancing security, efficiency, and transparency. These works examine decentralized banking, mobile payments, and DeFi applications, showcasing blockchain's potential to revolutionize financial transactions while addressing security and regulatory challenges.

Asmitha et al. [1] proposed a decentralized user wallet for digital banking, leveraging blockchain to enhance security and transparency. Their system employs CBC blockchain, where each transaction forms a cryptographically linked block, ensuring immutability. Using SHA-256 for password encryption and MD5 for PIN hashing, along with OTP verification, the framework strengthens access control. The model reduces transaction costs, eliminates intermediaries, and enhances trust in digital payments. This blockchain-based approach aims to revolutionize financial services by promoting decentralized and secure transactions.

Niturkar et al. [2] proposed a blockchain-based approach for banking transactions, eliminating tokens and unauthorized interference to enhance security. Their model replaces miners with a trusted architecture where only banks add blocks, ensuring controlled access. Using SHA-256 for hashing and verification, the system improves reliability while reducing delays. Simulations in NS-2 highlight better performance in delay, overhead, and throughput. This framework aims to create a transparent, efficient banking system by integrating decentralized blockchain technology.

Das et al. [3] proposed a blockchain-based security framework for mobile payments, enhancing transaction integrity through authentication, access control, and encryption. Their model ensures authorized access while preventing unauthorized interference, mitigating passive attacks and data tampering. By leveraging decentralization, the system strengthens security and availability. The study highlights encryption techniques and authentication workflows, emphasizing a multi-layered approach. This framework aims to improve mobile payment resilience, ensuring secure financial transactions while enhancing operational efficiency and user trust.

Naik et al. [4] proposed a blockchain-based approach to enhance banking security and efficiency. Their model eliminates intermediaries, using consensus mechanisms for secure fund transfers. Incorporating Java microservices and SHA-256 hashing, it improves transaction speed and mitigates fraud risks. Compared to traditional methods

like NEFT, the system reduces costs, enhances security, and streamlines operations. This framework aims to integrate blockchain into financial systems, ensuring regulatory compliance while optimizing banking transactions.

Akhilesh et al. [5] proposed a blockchain-based approach for secure banking, introducing a Proof-by- Approval consensus protocol to replace mining with an efficient validation mechanism. Their model ensures transaction integrity through cryptographic linking and SHA-256 hashing. By leveraging Hyperledger Fabric, the system enhances transparency while reducing costs and improving efficiency compared to traditional banking models. This framework aims to integrate blockchain technology into financial systems, offering a secure, scalable, and operationally feasible solution for banking transactions.

Meera et al. [6]analyzed how blockchain enhances financial transactions by improving security, transparency, and efficiency. Their research highlights the benefits of decentralization, removing intermediaries and ensuring tamper-proof records. Cryptographic techniques and hashing methods strengthen protections against fraud and cyber threats, making financial systems more resilient. The study also explores decentralized finance (DeFi), showcasing its ability to streamline banking operations and reduce costs, ultimately positioning blockchain as a transformative force in fintech and modern financial services.

These prior studies highlight blockchain's potential to enhance financial security, efficiency, and transparency. However, scalability and regulatory challenges persist. This study aims to develop an optimized framework for seamless financial integration and improved transaction integrity

Comparative Analysis

Sr. No	Authors	Title	Application	Methodology	Database	Evaluation Metrics	Performance
1	Asmitha M, Kavitha C.R.	Decentral- ized User Wallet: Transform- ing Digital Banking with Block- chain	Digital bank- ing, block- chain-based payment sys- tems	CBC block- chain, SHA- 256 encryp- tion, MD5 hashing, OTP verification	Not explic- itly men- tioned	Security measures (hashing, en- cryption, trans- action integ- rity)	Enhances se- curity, trans- parency, and decentraliza- tion in digital banking
2	Meera K L, Harshal Raje, C. Vijai, Rosy Kalia, Gau- tam Sen, Mohit Ti- wari	Using Blockchain technology for transpar- ent and se- cure Finan- cial Trans- actions in the Contem- porary Business Landscape	Transparent, tamper-proof financial transactions	Literature re- view, case study on SBI, SWOT analy- sis	SBI bank- ing data, various fi- nancial re- ports	Impact assess- ment based on user feedback (ease of KYC updates, fraud reduction, transaction ef- ficiency)	Enhanced fi- nancial secu- rity, decen- tralized fi- nance (DeFi), cost-effective transactions

3	Ramesh Cheripelli, D Marlene Garace Verghese, Ananda Kumar Reddy, K. Parijatha, Chilaka Chandana	Challenges and Opportunities of Blockchain in Financial Systems: The Impact of DeFi on Traditional Banking	Integration of blockchain in financial systems and DeFi's impact on traditional banking	Review of DeFi platforms, protocols, use cases; analysis of smart contracts, decentralized lending, yield farming	Not explicitly mentioned	Regulatory landscape evaluation, operational efficiency, accessibility, transparency comparison with traditional banking	Highlights DeFi's opportunities for financial innovation but also its challenges in security, scalability, and regulation
4	Lipsa Das, Chamandeep Kaur, Ayasha Siddiqua, Durdana Taranum, Ganesh Vasudeo Manerkar, Ajay Rana	Enhancing Security Of Mobile Payment Applications Using Blockchain	Security mechanisms for mobile payment applications	Authentication, access control, encryption techniques (RSA, AES/DES, ECC, PKI)	Various mobile payment platforms (Google Pay, Apple Pay, Paytm, BHIM, Samsung Pay)	Security metrics including confidentiality, integrity, non-repudiation	Strengthens security in mobile payment systems by preventing unauthorized access, ensuring data integrity, and reducing fraud risks
5	Shaliza Alwi, Irfah Najihah	Blockchain Technology Application	Exploring blockchain applications for banking	Literature review, security analysis,	Not explicitly mentioned	Security features assessment (decen-	Enhances transaction transparency, reduces fraud

	Basir Ma- lan, Siti Hawa Yusof, Ma- rina Mus- tafa	to the Bank- ing Sector	transactions	use case as- sessment for select bank- ing transac- tions		tralization, im- mutability, cryptographic security)	risks, im- proves effi- ciency in banking op- erations
6	Akhilesh Kumar Singh, Manish Raj	A Study of Analytics and Explo- ration of Bitcoin Challenges and Block- chain	Analytics and exploration of Bitcoin's impact and blockchain implementa- tion	Literature re- view, eco- nomic study of Bitcoin adoption, analysis of blockchain architecture, security con- cerns	Economic reports, cryptocur- rency mar- ket data	Bitcoin net- work security evaluation, li- quidity risks, economic scalability	Explores Bitcoin's po- tential for fi- nancial dis- ruption while identifying challenges in security, mar- ket stability, and adoption
7	Niturkar Pallavi Pravin, Ku- lat Pratik- sha Anil, Sukate Ma- nasi Sunil, Modhave Snehal Kundlik, Phalke Akshay Su- has	Blockchain Technology for Protect- ing Banking Transac- tions With- out Using Tokens	Secure bank- ing transac- tions without token-based validation	SHA-256 hashing, con- sensus proto- cols, proof- of- work, de- centralized validation	Not explic- itly men- tioned	Delay, over- head, and throughput analysis	Demonstrates enhanced se- curity and ef- ficiency for banking transactions by eliminat- ing token de- pendence
8	Varsha Naik, Riya Pejawar, Rishabh Singh, Prof. Anagha Aher, Prof. Sneha Kan- chan	Expeditious Banking Using Blockchain Technology	Secure and efficient fund transfer in banking sys- tems	Blockchain- based decen- tralized NEFT, Java micro- services, IFSC integra- tion	Not explic- itly men- tioned	Consensus ef- ficiency, trans- action security, decentraliza- tion impact	Enhances banking effi- ciency by re- ducing fraud, eliminating third-party intervention, and ensuring secure fund transfers
9	Akhilesh NS, Aniruddha MN, Sowmya K S	Implemen- tation of Blockchain for Secure Bank Trans- actions	Secure bank- ing transac- tions using blockchain technology	Introduction of Proof-by- Approval protocol, lit- erature re- view of blockchain consensus models (PoW, PoS, PoR).	Not explic- itly men- tioned	Comparison of Proof-by-Ap- proval vs. tra- ditional PoW/PoS con- sensus models	Establishes an alternative consensus protocol im- proving secu- rity while re- ducing en- ergy costs in blockchain- based bank- ing

Expected Results

1. **Enhanced Transaction Security**
The system employs modern cryptographic techniques (e.g., bcrypt, Argon2, AES-GCM) to secure user credentials and financial data, significantly reducing the risk of data breaches and brute-force attacks.
2. **Stronger User Authentication**
Time-based two-factor authentication (TOTP) is used for both login and transactions, offer- ing better protection against phishing and unauthorized access compared to traditional email- based verification.
3. **Tamper-Proof Transaction Logging**
A private blockchain structure ensures all transaction records are immutable and verifiable, providing a secure audit trail for detecting fraud and maintaining data integrity.
4. **Real-Time Fraud Detection**
Machine learning algorithms analyze transaction behavior continuously to identify anoma- lies, helping prevent fraudulent activities in real-time.

Conclusion

The shift from centralized banking to decentralized blockchain solutions brings improved security, transparency, and user control. The proposed system uses modern cryptographic methods like bcrypt/Argon2 for hashing and AES-GCM/ChaCha20 for encryption to protect user data, along with TOTP-based two-factor authentication and hash chained logs to ensure secure access and tamper-proof records. Designed for efficient performance even on low power devices, it also features a modular structure and support for post-quantum cryptography, making it adaptable to future security challenges. Together, these enhancements create a secure, scalable, and user-friendly blockchain wallet that supports a safer and more efficient digital banking experience.

References

[1]A. M and C. R. Kavitha, “Decentralized User Wallet: Transforming Digital Banking with Blockchain,” in Proc. 8th Int. Conf. on IoT in Social, Mobile, Analytics and Cloud (I SMAC), 2024,
pp. 566–571.

[2]M. K. L, H. Raje, C. Vijai, R. Kalia, G. Sen, and M. Tiwari, “Using Blockchain Technology for Transparent and Secure Financial Transactions in the Contemporary Business Landscape,” in Proc. 2024 Int. Conf. on Trends in Quantum Computing and Emerging Business Technologies (TQCEBT), 2024, pp. 1–4.

[3]R. Cheripelli, D. M. G. Verghese, A. K. Reddy, K. Parijatha, and C. Chandana, “Challenges and Opportunities of Blockchain in Financial Systems: The Impact of DeFi on Traditional Banking,” in Proc. 4th Int. Conf. on Mobile Networks and Wireless Communications (ICMNWC), 2024, pp. 1–8.

[4]L. Das, C. Kaur, A. Siddiqua, D. Taranum, G. V. Manerkar, and A. Rana, “Enhancing Security Of Mobile Payment Applications Using Blockchain,” in Proc. 10th IEEE Uttar Pradesh Section Int. Conf. on Electrical, Electronics and Computer Engineering (UPCON), 2023, pp. 210–214

[5]S. Alwi, I. N. B. Malan, S. H. Yusof, and M. Mustafa, “Block Chain Technology Application to the Banking Sector,” in Proc. 2023 Int. Conf. on Artificial Intelligence and Smart Communication (AISC), 2023, pp. 817–821.

[6]A. K. Singh and M. Raj, “A study of Analytics and Exploration of Bitcoin Challenges and Blockchain,” in

Proc. Int. Conf. on Electronics and Renewable Systems (ICEARS), 2022, pp. 929– 933.

[7]P. Niturkar, P. Kulat, M. Sukate, S. Modhave, and A. Phalke, "Blockchain technology for protecting banking transactions without using tokens," in Proc. 2nd Int. Conf. on Inventive Research in Computing Applications (ICIRCA), 2020, pp. 801–807.

[8]V. Naik, R. Pejawar, R. Singh, A. Aher, and S. Kanchan, "Expeditious Banking Using Blockchain Technology," in Proc. IEEE Int. Conf. on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE), 2020, pp. 566–571.

[9]A. NS, A. MN, and S. K S, "Implementation of Blockchain for Secure Bank Transactions," in Proc. Int. Conf. on Mainstreaming Blockchain Implementation (ICOMBI), 2020, pp. 1–15.

[10]S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Decentralized Business Review, vol. 1, pp. 212–219, 2008.

[11]M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," Applied Innovation Review, vol. 2, no. 6–10, 2016.

[12]K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[13]L. Chen, L. Xu, Z. Shah, and Z. Gao, "A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems," in Proc. 22nd Int. Conf. on Parallel and Distributed Systems (ICPADS), 2022, pp. 564–571.

[14]A. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards Blockchain-Based Auditable Storage and Sharing of IoT Data," in Proc. 2017 on Cloud Computing Security Workshop (CCSW), ACM, 2017, pp. 45–50.

[15]G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in Proc. IEEE Security and Privacy Workshops (SPW), 2015, pp. 180–184.

Copyright & License:
© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.