American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

BLOCKCHAIN-BASED FRAMEWORK FOR SECURE AND EFFICIENT FINANCIAL TRANSACTIONS

DR. D. BHADRU[1], A. SAI KUMAR[2], S. CHANDANA[3], P. SIRI HAKSHITHA[4], PINJA ADITHYA[5]

ASSOCIATE PROFESSOR[1], UG SCHOLAR[2,3,4&5]

DEPARTMENT OF AI&ML, NARSIMHA REDDY ENGINEERING COLLEGE (UGC- AUTONOMOUS) MAISAMMAGUDA (V), KOMPALLY, SECUNDERABAD, TELANGANA-500100

ABSTRACT

The increasing digitization of the banking sector has brought about significant advancements in customer service and transaction efficiency. However, this evolution has also introduced a range of security challenges, particularly concerning data privacy, transaction integrity, and vulnerability to cyber threats. Traditional e-banking systems, though efficient, are often susceptible to security risks such as phishing, malware attacks, and data breaches, which can compromise sensitive financial information and undermine customer trust. In response to these challenges, blockchain technology has emerged as a revolutionary solution that provides enhanced security, transparency, and decentralization, making it highly suitable for secure banking applications. This project, Secure Banking Using Blockchain, aims to explore the potential of blockchain technology in mitigating the security risks associated with online banking systems. By leveraging blockchain's decentralized architecture, cryptographic principles, and consensus mechanisms, this research seeks to provide a more secure and transparent banking environment. The study begins by reviewing the current state of traditional e-banking systems, identifying their vulnerabilities, and analyzing the security methods currently implemented by banks. Surveys and archival data are utilized to understand customer and banker perspectives on adopting blockchain-based solutions, with security emerging as the core concern for both groups. The research further explores various categories of threats specific to both traditional and blockchain banking systems, such as phishing, hacking, Distributed Denial of Service (DDoS) attacks, smart contract vulnerabilities, and 51% attacks. A comparative study of existing security protocols in traditional systems (e.g., SSL, HTTPS) and blockchain mechanisms (e.g., encryption, digital signatures, consensus algorithms like Proof of Work and Proof of Stake) is conducted. The focus is on how blockchain's immutable ledger, decentralized control, and cryptographic methods offer significant advantages in mitigating these threats. Two blockchain-based encryption algorithms are presented as part of the project. The first algorithm, NPN (Prime Numbers and Pseudo-Random Number Generator), combines cryptographic techniques to enhance the security of banking transactions by ensuring unpredictability and randomness in encryption keys. The second algorithm, LIE architecture, leverages a multi-round encryption process based on the Fiestel network, utilizing a set of discrete cryptographic sub-keys and permutation matrices to provide robust data security. The LIE algorithm also applies the blockchain principles of confusion and diffusion to maximize the difficulty of data manipulation and enhance transaction integrity. Additionally, the research highlights the mathematical underpinnings of these algorithms, such as XOR operations, multiplication, and cryptographic hashing, which are critical to achieving essential properties like avalanche effects, statistical independence, and completeness. Both algorithms are designed to meet the stringent security demands of modern banking systems, ensuring that sensitive data remains secure during transactions. To validate the performance and effectiveness of the proposed algorithms, a comparative analysis is conducted with existing blockchain encryption methods. The time and space complexity of the designed algorithms are optimized and evaluated to ensure they are both efficient and scalable for real-world banking applications. The project concludes with recommendations for implementing blockchain-based security in modern banking systems, focusing on preventive measures to protect data from hacking, corruption, or unauthorized alteration. By proposing innovative cryptographic algorithms and optimizing their performance, this project contributes to the growing body of research on blockchain security in the financial sector and provides a practical framework for enhancing the security of online banking transactions.

INTRODUCTION

Bank has been originated from Banco, which is an Italian word which means bench (all transactions were conducted while sitting on the bench) (yousigma.com). Originally, the Jews and later the goldsmiths were involved in money lending. Banks being financial organization were initially involved in depositing and lending of money. Banks now offer various facilities like accepting deposits, lending loans, credit/ debit card, foreign exchange, locker facility, paying bills and dues, ACH (Automated Clearing House), ECS (Electronic Clearance Service), etc. Banks are growing tremendously in terms of making cashless or digital transactions. Individuals, business house, corporates, etc. transact with banks. Human always had the zeal to progress & improve the existing technologies. Technology has led to great development and growth, which has given a platform for further developments. Earlier, Traditional Bank had a physical branch (brick and mortar model), where the customers can directly visit and meet bank staff in person. Later, the facility of inquiring about the account information was handled via phone also popularly known as Phone Banking. Gradually ATMs (Automated Teller Machines) were introduced which made the life of bankers and customers very convenient. Customers can draw money anytime without worrying about the branch timings, and holidays of a bank by using ATM. With the innovation in information technology the development and availability of resources like internet speed has helped the customers to use the banking services 24*7 anywhere, anytime with a lot of ease. The Internet

Received: 13-02-2026 | Accepted: 21-03-2026 | Published: 27-03-2026

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

is one of the great advancement accomplished by humankind till date. The Internet has influenced different aspects of society. Through internet; the user can view stock market details, news, sports, and results of an examination, & can also access bank account, shop, communicate etc. Banking domain is extensively using and growing with the internet; they are offering various financial services online. The Internet offers significant benefits to society but also leaves various loopholes for severe crime. Dealing with the finances and customer-centric data; banking industry has turned into databank of sensitive information. Especially now, when customers are paying electronically through e-banking or any third party website, the banks needs security for the customers' data and the transactions. The banks have successfully implemented E-Commerce (Kardaras and Papathanassiou, 2001). In India, after demonetisation, the government is promoting digital India campaign. The banks & business houses are advised to keep modes of e-payments may be by APPs or POS machines or third party payment options. Internet banking denotes the services offered remotely via bank on their website or now a days mobile apps (Suganthi, 2001; Dannenerg and Kellner, 1998; Zineldin, 1995). It is the fastest, easiest and efficient way of banking compared to traditional methods. Technology has instigated as a tactical resource for banks in attaining higher competence, managing the processes, increasing the efficiency & profitability. For customers, the ease & speed to access their bank 24*7 all through the year and from any location is a very lucrative option. To sustain in the world of digitization, all industry including banks have been prompt to accept & use the technology in the best ways. Internet banking services are critical to handle customer demands, to enhance customer relationship management, face competition, and ensure better security. Banks requires relatively very less investment for e-banking as compared to traditional branch banking (brick & mortar model) (Burnham, 1996). Services offered Online by banks- banking is maturing with time, initially the banks website used to be only informative, later the customers' were given login credentials to check the balance and transaction history online, now various services like paying bills online, transfer money across different accounts, apply for loan online, shop online via credit/debit/net banking, etc. are available. Banks are launching the Mobile Apps with enhanced features like biometric for making online transactions more secure.

LITERATURE REVIEW

Blockchain technology has gained significant attention in financial systems due to its ability to provide **secure, transparent, and efficient transaction processing**. Researchers have explored different blockchain architectures, consensus mechanisms, and cryptographic techniques to improve the reliability and performance of financial transaction systems.

Blockchain Technology in Financial Services

Blockchain is a **distributed ledger technology** that records transactions across multiple nodes, ensuring transparency, immutability, and trust without relying on centralized authorities. Several studies highlight that financial institutions increasingly adopt blockchain to enhance **authentication, transparency, and risk management** in digital transactions. The technology can simplify clearing and settlement processes while maintaining accurate financial records.

Research shows that blockchain improves the efficiency of financial systems by enabling **peer-to-peer transactions, digital identity management, and smart contracts**. These features reduce operational costs and eliminate the need for intermediaries in financial transactions.

Security Improvements in Blockchain-Based Transactions

Security is one of the most important advantages of blockchain systems. Blockchain uses **cryptographic hashing, digital signatures, and distributed consensus mechanisms** to ensure the integrity and authenticity of transaction records. Studies indicate that blockchain systems provide strong protection against fraud, unauthorized access, and data tampering, making them suitable for secure financial applications.

Researchers have also explored enhanced cryptographic mechanisms such as **Zero-Knowledge Proofs and advanced verification methods** to improve the privacy and efficiency of blockchain networks. These techniques reduce computational overhead while maintaining strong security guarantees.

Blockchain for Efficiency and Performance Optimization

Traditional financial systems often suffer from **slow transaction processing, high transaction costs, and reliance on centralized authorities**. Blockchain technology addresses these challenges through decentralized transaction validation and automated smart contracts.

Recent studies propose **hybrid consensus protocols** combining Proof-of-Stake (PoS) and Byzantine Fault Tolerance (BFT) to improve transaction speed, reliability, and scalability in blockchain networks. These approaches enhance both security and operational efficiency in financial transaction systems.

Furthermore, blockchain-based financial platforms enable **real-time settlement, transparent record keeping, and automated transaction verification**, which significantly improves the performance of digital financial services.

Applications of Blockchain in Financial Transactions

Many financial sectors have started integrating blockchain technology to improve transaction security and transparency. Applications include:

- **Cryptocurrency transactions and digital payments**
- **Cross-border payment systems**

Received: 13-02-2026 | Accepted: 21-03-2026 | Published: 27-03-2026

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

- **Smart contracts for automated financial agreements**
- **Fraud detection and secure financial auditing**
- **Decentralized finance (DeFi) platforms**

Studies also show that blockchain improves financial service quality by enhancing **trust, transparency, and data integrity in digital financial ecosystems**.

Challenges and Research Gaps

Despite its advantages, blockchain adoption in financial transactions still faces several challenges:

- **Scalability limitations in large-scale financial networks**
- **High computational cost and energy consumption**
- **Regulatory and compliance challenges**
- **Potential vulnerabilities such as transaction manipulation attacks**

These limitations highlight the need for **advanced blockchain frameworks that balance security, scalability, and efficiency** in financial transaction systems.

SYSTEM ANALYSIS

EXISTING SYSTEM

Traditional financial transaction systems are mainly based on **centralized banking and payment infrastructures**. These systems rely on **intermediaries such as banks, payment gateways, and clearing houses** to process and validate financial transactions. While these systems are widely used, they suffer from several limitations related to **security, transparency, and processing efficiency**.

In the existing system, transaction data is stored in **centralized databases**, making them vulnerable to **cyberattacks, data breaches, and unauthorized modifications**. Additionally, cross-border transactions often involve multiple intermediaries, which increases **transaction costs, processing time, and operational complexity**.

Traditional systems also lack **full transparency and traceability**, making it difficult to verify transactions or detect fraudulent activities in real time. Delays in transaction settlement and dependency on trusted third parties further reduce system efficiency.

Limitations of Existing System

- Dependence on **centralized financial institutions**.
- Higher risk of **data breaches and cyberattacks**.
- **Slow transaction processing**, especially for international payments.
- **High operational and transaction costs** due to intermediaries.
- Limited **transparency and traceability** in transaction records.
- Difficulty in detecting **fraudulent transactions** in real time.

PROPOSED SYSTEM

The proposed system introduces a **blockchain-based framework** to enhance the **security, transparency, and efficiency of financial transactions**. Blockchain technology uses a **decentralized distributed ledger**, where transaction records are securely stored across multiple nodes in the network.

In this system, every financial transaction is **validated through consensus mechanisms** and recorded as a block in the blockchain. Once added, the transaction data becomes **immutable and tamper-resistant**, ensuring high levels of security and trust.

The proposed framework also utilizes **smart contracts**, which automatically execute predefined rules for financial transactions without requiring intermediaries. This reduces processing delays and operational costs while improving transaction efficiency.

Additionally, blockchain provides **end-to-end transparency**, allowing authorized participants to track transactions in real time. Advanced **cryptographic techniques** ensure data privacy and secure authentication for users.

ADVANTAGES OF PROPOSED SYSTEM

- **Decentralized transaction processing** without intermediaries.
- Enhanced **security using cryptographic algorithms**.
- **Immutable transaction records** preventing data tampering.
- Faster transaction processing and settlement.
- Reduced operational and transaction costs.
- Improved **transparency and traceability** of financial transactions.
- Smart contract automation for secure and efficient operations.

IMPLEMENTATION

The proposed blockchain-based banking system is designed to provide a secure and efficient environment for processing transactions. The architecture is divided into several components:

- **Blockchain Network**: A private Ethereum blockchain network, simulated using **Ganache**, serves as the

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

backbone of the system. It records and stores all transaction data, ensuring transparency and security.

- **Smart Contracts**: Smart contracts automate various banking processes, such as executing transactions, verifying identities, and enforcing compliance with security protocols.
- **MetaMask Wallet**: **MetaMask** acts as the interface between users and the blockchain network. It is used for signing and executing transactions securely, ensuring that only authorized users can access the system.
- **Web Application**: A web-based interface allows users such as bankers and customers to interact with the system securely. It provides modules for account management, transaction monitoring, and auditing.

System Design and Development

The development of the secure banking system follows a structured approach involving several phases: requirement analysis, system design, smart contract development, web application development, and testing.

Requirement Analysis

This phase involves understanding the key security challenges of traditional banking systems and identifying how blockchain can resolve these issues. The following requirements were identified:

- **Authentication and Authorization**: Ensure that only authorized users can access or modify data.
- **Transaction Security**: Provide end-to-end encryption and immutability for all transactions.
- **Data Privacy**: Protect sensitive customer information through cryptographic methods.
- **Regulatory Compliance**: Ensure the system complies with banking regulations and financial standards.

System Design

Based on the requirements, the system's architecture is divided into the following layers:

- **Blockchain Layer**: The private Ethereum blockchain simulated using **Ganache** stores transaction data.
- **Smart Contract Layer**: Smart contracts manage transaction processes, such as identity verification and fund transfers.
- **Application Layer**: A web-based application provides the user interface for interacting with the blockchain.
- **Integration Layer**: This layer consists of APIs that enable communication between the web application, MetaMask wallet, and the blockchain.

Smart Contract Development

Smart contracts are written in **Solidity**, the primary programming language for developing smart contracts on Ethereum. The contracts automate core banking operations such as:

- **Transaction Processing**: Securing and recording every transaction on the blockchain.
- **Identity Verification**: Verifying user credentials and ensuring that only authenticated users can access their accounts.
- **Compliance Checking**: Ensuring that every transaction complies with banking regulations.

Each smart contract is tested using the **Truffle** framework to ensure that it functions as intended and is secure before being deployed on the blockchain network.

Web Application Development

The web application is developed using **React.js** to provide a user-friendly interface for customers and banking staff. The application is designed to handle:

- **Customer Module**: Allows customers to manage accounts, view transaction history, and initiate transactions.
- **Banker Module**: Enables bank staff to verify transactions, monitor security issues, and manage customer accounts.
- **Admin Module**: Provides system administrators with tools to oversee the entire system, ensuring compliance and security.

The application integrates with **MetaMask** to securely sign and manage transactions.

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

Implementation and Deployment

The implementation of the medicine supply chain management system involves deploying the smart contracts on the private Ethereum blockchain network and hosting the web application on a web server.

Ganache Setup

Ganache is set up to simulate a private Ethereum blockchain network on a local machine. It provides a graphical interface for managing accounts, viewing transactions, and monitoring smart contract events. The blockchain network is configured to have multiple accounts, each representing a different stakeholder in the supply chain, such as manufacturers, distributors, pharmacists, and consumers.

Smart Contract Deployment

The smart contracts are deployed on the Ganache blockchain network using the Truffle framework. Truffle provides a suite of tools for compiling, deploying, and managing smart contracts. The deployment script is configured to deploy all the smart contracts to the blockchain network and initialize them with the necessary data.

MetaMask Integration

MetaMask is integrated with the web application to provide a secure and convenient way for users to interact with the blockchain network. Users are required to install the MetaMask extension in their browser and create a wallet. The web application is configured to connect to the Ganache blockchain network using MetaMask, allowing users to sign transactions and execute smart contracts.

Web Application Deployment

The web application is deployed on a web server using a platform-as-a-service (PaaS) provider, such as Heroku or AWS Elastic Beanstalk. The application is configured to connect to the Ganache blockchain network using Web3.js, a JavaScript library for interacting with the Ethereum blockchain. The deployment process involves building the application, configuring environment variables, and setting up a domain name.

CONCLUSION The implementation of blockchain technology in the banking sector has the potential to significantly enhance the security, transparency, and efficiency of financial transactions. By decentralizing the management of transactions and removing the need for trusted third-party intermediaries, blockchain introduces a new level of trust through its cryptographic security, distributed ledger, and immutable record-keeping. In this project, **secure banking using blockchain** was demonstrated as a viable solution for addressing the shortcomings of traditional banking systems, such as inefficiencies, high operational costs, data breaches, and mistrust in centralized institutions. Blockchain ensures that each transaction is verified, transparent, and secure, eliminating the possibility of tampering or fraud. Furthermore, the introduction of smart contracts can automate complex banking operations, improving operational efficiency and reducing the need for human intervention. Despite the significant benefits, the technology is not without its limitations. Challenges such as ensuring the accuracy of the initial data input, potential vulnerabilities in smart contract programming, and scalability issues must be addressed before blockchain can be fully integrated into mainstream banking systems. However, as advancements continue, blockchain's capability to deliver secure, real-time, and auditable transactions could revolutionize banking and redefine how trust is established in financial services. In conclusion, blockchain technology presents a transformative opportunity for secure banking, fostering a future where financial transactions are more transparent, secure, and efficient. With continued innovation and collaboration in this field, blockchain could play a critical role in shaping the future of banking and restoring trust in the financial system.

REFERENCES

1. Antonopoulos, A.M. Cryptocurrency Transaction Speeds: The Complete Review. Available online: https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch01.html (accessed on 25 June 2022).

2. Scribe, G.A. Understanding Cryptocurrency Transaction Speeds. Available online: https://medium.com/coinmonks/understanding-cryptocurrency-transaction-speeds-f9731fd93cb3 (accessed on 25 June 2022).

3. Jaoude, J.A.; Saade, R.G. Blockchain Applications—Usage in Different Domains. IEEE Access **2019**, 7, 45360–45381. [CrossRef]

4. Shahbandi, M. Financial Technologies for Accepting Transactions Using Blockchain Technology and Crypto Currency

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

in Digital Marketing. Int. Bus. Econ. Stud. **2021**, 3, 23. [CrossRef]

5. Bonneau, J.; Miller, A.; Clark, J.; Narayanan, A.; Kroll, J.; Felten, A. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 17–21 May 2015.

6. Eberhart, R.; Kennedy, J. A New Optimizer using Particle Swarm Theory. MHS'95. In Proceedings of the Sixth International Symposium on Micro Machine and Human Science, Nagoya, Japan, 4–6 October 1995.

7. Feng, L.; Zhang, H.; Tsai, W.T. System architecture for high-performance permissioned blockchains. Front. Comput. Sci. **2019**, 13, 1151–1165.

8. Amine, M.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the internet of things: Research issues and challenges. IEEE Internet Things J. **2018**, 6, 2188–2204.

9. Fu, Z.; Dong, P.; Li, S.; Ju, Y. An intelligent cross-border transaction system based on consortium blockchain: A case study in Shenzhen, China. PLoS ONE **2021**, 16, e0252489. [CrossRef]

10. Gartner. Blockchain Potential and Pitfalls. Available online: https://www.gartner.com/en/webinars/3878710/blockchainpotential- and-pitfalls (accessed on 2 March 2022).

11. Kamal, H.; Moussa, D.; Batrick, S. A Comparative Study of Various Metaheuristic Techniques Applied to The Multilevel Thresholding Problem. Eng. Appl. Artif. Intell. **2010**, 23, 676–688.

12. Huang, K.; Zhang, X.; Mu, I.; Rezaeibagha, F.; Du, X.; Guizani., N. Achieving intelligent trust-layer for internet-of-things via self-redactable blockchain. IEEE Trans. Ind. Inform. **2019**, 16, 2677–2686. [CrossRef]

13. Huemer, C.; Liegl, P.; Zapletal, M. Handbook of e-Tourism; Springer: Berlin/Heidelberg, Germany, 2022; pp. 343–371.

14. Khacef, K.; Pujolle, G. Web, Artificial Intelligence and Network Applications; Springer International Publishing: Cham, Switzerland, 2019; pp. 662–672.

15. Klapita, V. Implementation of electronic data interchange as a method of communication between customers and transport company. Transp. Res. Procedia **2021**, 53, 174–179. [CrossRef]