International Journal of Computer Techniques–IJCT Volume 12 Issue 6, November 2025

Open Access and Peer Review Journal ISSN 2394-2231 https://ijctjournal.org/

Secure Blockchain Transaction: A Literature Survey

Authors:

ANANYA.N (ananyapoojari7795@gmail.com)

GREESHMA. M.S (greeshmavara2004@gmail.com)

PANCHAMI. G (panchami0120@gmail.com)

VANDHANA. K.M (vandanagowda86@gmail.com)

Guide:

Rakshitha. P

Assistant Professor, Department of Cybersecurity

Sri Venkateshwara College of Engineering, Banglore-562157

Abstract:

In today's era of digital transformation, online transactions have become vital to financial systems, e-commerce, and decentralized applications. However, increasing dependence on digital payment infrastructures has also raised major security concerns such as hacking, identity theft, and unauthorized access. To address these challenges, the proposed project **"Blockchain Secure Transaction"** presents a decentralized framework that ensures transparency, integrity, and confidentiality in digital transactions. The system uses blockchain technology to record and validate each transaction in a distributed ledger, eliminating centralized control and making data immutable and tamper-proof.

The workflow begins with user registration, where users provide details and set a picture password for secure recognition. During login, the system verifies credentials and performs biometric authentication to confirm user identity. Unregistered users are redirected to the registration page, maintaining process integrity. Once authenticated, users access the dashboard to initiate secure transactions.

To preserve privacy, Zero-Knowledge Proof (ZKP) is used, allowing users to prove transaction authenticity without revealing sensitive information. Transactions then pass through smart contract verification, which ensures compliance with predefined conditions. Successful verifications result in completed transactions, while suspicious or invalid ones are blocked or frozen automatically.

All user data and transaction logs are securely stored in Firebase, with backend processing handled in Java and the frontend designed using React (app.jsx). By combining blockchain's immutability, smart contract automation, ZKP privacy proofs, and biometric authentication, the Blockchain Secure Transaction System offers a multi-layered, tamper-resistant, and transparent solution for secure online payments — enhancing trust and reliability in the digital economy.

1. Introduction:

As technology advances, financial transactions are increasingly being executed through online platforms, e-banking systems, and decentralized networks. Although these systems provide speed and convenience, they also create multiple security challenges including data breaches, impersonation attacks, and unauthorized fund transfers. Centralized systems are especially prone to attacks since a single point of failure can compromise an entire network. To counter

these challenges, blockchain technology has emerged as a revolutionary solution that ensures data immutability, decentralization, and traceability of every transaction.

The proposed Blockchain Secure Transaction System aims to deliver a fully decentralized and transparent platform for secure digital payments and data exchange. Unlike traditional systems, it does not rely on a central server but instead distributes transaction records across multiple nodes. Every transaction is verified through consensus mechanisms, making it virtually impossible for attackers to alter or delete records.

The system architecture begins with a registration phase, where a new user creates an account and sets a picture password—a graphical authentication technique that enhances usability and security. Upon attempting to log in, the system validates credentials; if the user is unregistered, it redirects back to the registration page. After successful login, the system employs biometric verification to confirm user identity, adding an additional layer of protection. Once verified, the user is directed to the dashboard, which serves as the central control hub for viewing transaction history and initiating new transactions.

When a transaction is initiated, it passes through a Zero-Knowledge Proof (ZKP) phase. ZKP enables one party to prove the legitimacy of information (e.g., account ownership or transaction validity) to another without revealing sensitive data. This ensures privacy even during verification. The transaction is then processed through smart contracts that check compliance with security and rule-based conditions. If all verifications succeed, the transaction status is updated as successful and recorded immutably on the blockchain. However, if any inconsistency, unauthorized access, or mismatch is detected, the system immediately blocks or freezes the transaction, preventing any fraudulent activity.

All sensitive data—including user credentials, biometric templates, and picture passwords—are securely stored in Firebase, protected with encryption and authentication layers. The backend processes, coded in Java, handle ZKP computations and blockchain integration, while the user interface built with React (app.jsx) ensures a seamless experience across all stages: registration, login, authentication, and transaction monitoring.

In essence, this project demonstrates how combining blockchain, ZKP, biometric authentication, and smart contracts can establish a highly secure, privacy-preserving transaction environment. It ensures that every transaction is verified, traceable, and tamper-proof, thereby providing complete trust and reliability to users. The Blockchain Secure Transaction System thus represents the next generation of secure digital transaction frameworks—offering resilience, transparency, and confidence in every exchange

1.1. Problem Statement and Objectives:

The proposed project titled **“Blockchain Secure Transaction”** focuses on developing a decentralized and highly secure transaction system that ensures transparency, integrity, and data privacy. The main goal of this project is to overcome the limitations of traditional centralized transaction systems by implementing blockchain technology, which provides an immutable and tamper-proof ledger for recording transactions. The system integrates multiple layers of security, including picture password**,** biometric authentication**,** smart contracts, and Zero-Knowledge Proof (ZKP)**,** to protect user identities and prevent unauthorized access. It also ensures that every transaction is verified through blockchain and smart contract mechanisms, maintaining trust and accountability.

The key objectives of this project are to design a blockchain-based secure framework for online transactions, enhance user authentication using biometrics and picture passwords, employ ZKP

for privacy-preserving verification, automate transaction validation through smart contracts, and immediately block or freeze any suspicious or unauthorized transaction.

Through these objectives, the Blockchain Secure Transaction System aims to provide a reliable, transparent, and privacy-focused solution for modern digital payments.

1.2. Objective of the Study:

The primary objectives of this literature survey and the subsequent project are as follows:

1. **To develop a** blockchain-based secure transaction system that ensures transparency, confidentiality, and data integrity.
2. **To design a decentralized framework** that removes dependency on centralized servers and prevents tampering or data manipulation.
3. **To implement multi-factor authentication** using picture passwords and biometric verification for enhanced user security.
4. **To integrate Zero-Knowledge Proof (ZKP)** for privacy-preserving authentication and transaction validation.
5. **To utilize smart contracts** for automated and trustworthy verification of transactions.
6. **To ensure that any unauthorized** or suspicious transaction is automatically blocked or frozen to prevent fraud.
7. **To store user data and transaction** details securely using Firebase and implement backend processing in Java for system reliability.
8. **To provide a user-friendly interface** through React (app.jsx) for smooth navigation from registration to transaction completion.

1.3. Methodology:

The methodology begins with user registration, followed by setting a picture password and performing login authentication. Unregistered users are redirected back to the registration page. After successful biometric verification, users access the dashboard to initiate transactions. Each transaction passes through Zero-Knowledge Proof (ZKP) and verification stages; if verified, it becomes a successful transaction, otherwise it is blocked or frozen to ensure system security.

1.3.1. Research Approach:

The Blockchain Secure Transaction project was developed in 2025 using a practical and step-by-step approach. I first designed the system flow including registration, login, biometric, and transaction processes. Then I implemented security features like Zero-Knowledge Proof (ZKP) and smart contracts for safe verification. Finally, I used Java, Firebase, and React (app.jsx) to build a secure and user-friendly system.

1.3.2. Source of Data:

The following sources were used to gather literature:

1. IEEE Xplore, SpringerLink, and ScienceDirect journals for research papers related to blockchain security, smart contracts, and Zero-Knowledge Proof (ZKP).

2. Publications and articles from renowned institutions such as MIT, Stanford University, and other global research organizations focusing on decentralized systems and cybersecurity.
3. Official blockchain documentation, developer forums, and online resources for understanding practical implementation using Java, Firebase, and React (app.jsx).

1.3.3. Keyword Strategy:

The keywords used were Blockchain Security, Smart Contracts, Zero-Knowledge Proof (ZKP), Decentralized Transactions, and Biometric Verification to gather relevant information for the project.

1.3.4. Selection Criteria:

Selection was based on:

1. **Focus Area:** Selected studies that directly relate to blockchain security, smart contracts, Zero-Knowledge Proof (ZKP), and secure transaction systems.
2. **Time Frame:** Preference was given to research works published after 2020 to include the most recent technological advancements.
3. **Source Quality:** Chosen from peer-reviewed journals, top conference papers, and recognized industry publications to ensure accuracy and reliability.

1.4. Literature Survey:

This section reviews studies and technologies related to blockchain security, smart contracts, and ZKP, forming the base for the Blockchain Secure Transaction project.

Source (Year)	Focus / Objective	Techniques Discussed	Key Contributi-ons / Findings	Context / Applicati-ons	Challenge /Limitatio ns	Relation / Gap vs. Blockchain Secure Transaction
Abubakar et al., 2023 (IET Research Journal)	Improve accuracy of blockchain -based intrusion detection	Blockchain-assisted IDS, distributed ledger, encryption	Proposed a tamper-proof intrusion detection system using blockchain	Distribute-d networks / security	Scalability , on-chain storage cost	Related in blockchain-based security, but your project focuses on transaction verification with ZKP and authentication layers, not IDS.
Shalabi, 2024 (ScienceD irect)	Review of blockchain -based IDS/IPS for IoT	Blockchain consensus, decentralized validation	Showed blockchain can ensure secure IoT communicat -ion	IoT/IIoT security	High data volume, system overhead	Uses blockchain for IDS; your system extends it for transaction flow and user authentication security.

Zhou et al., 2024 (ScienceDirect)	Improve privacy in blockchain identity and transaction	zk-SNARKs, zk-STARKs, commitments	Enabled privacy-preserving identity verification	Blockchain identity and secure transaction	High proof computation cost	Supports your ZKP approach; you extend it by integrating biometrics, picture password, and OTP for end-to-end verification.
Zhang et al., 2024 (MDPI)	Privacy-preserving data trading using blockchain & ZKP	Smart contracts, ZKP commitments	Enabled secure, auditable data exchanges	Private data marketplc-es	Verification cost, off-chain proof issues	Similar ZKP logic; your project applies it to financial transactions with dashboard and freeze/block mechanism.
Vidal, 2024 (ScienceDirect)	Review of smart contract vulnerabili-ty detection	Static analysis, contract auditing	Summarized automated methods to secure contracts	Smart contract-based systems	Limited coverage, false positives	Supports secure contracts; your system uses secure contracts for automatic transaction control and blocking failures.
Research Survey, 2024 (Research Gate)	Evaluate detection of smart contract flaws	Formal verification, static & dynamic analysis	Compared multiple detection tools	Blockchain auditing	Code complexity, limited automation	Focused on contract analysis; your project builds on verified contracts but adds user-level authentication and ZKP validation.
Li et al., 2023 (Data Science Journal)	Privacy-preserving IDS using blockchain	Secure node validation, ledger logging	Proposed decentralized IDS model using blockchain	Cross-organization IDS	Communication overhead	Focuses on IDS, while your project targets secure transactions and user authentication flow.
Chu et al., 2024 (Technical Report)	Detect and mitigate smart contract flaws	Static analysis, code auditing	Enhanced vulnerability detection for contracts	Blockchain smart contracts	Complexity for large projects	Related in contract verification; your work extends security by adding ZKP and biometric authentication layers.

Li & Q., 2025 (ACM Digital Library)	Blockchain collaborative IDS for critical systems	Blockchain logging, alert propagation	Improved security via distributed alert sharing	Critical infrastructure	Real-time alert delay	You apply blockchain differently — for secure user transactions, not network intrusion detection
VS et al., 2025 (ScienceDirect – Expert Systems Applications)	Secure IIoT transactions through blockchain validation	Smart contract monitoring, blockchain ledger	Provided decentralized validation for IIoT systems	Industrial IoT security	Latency, low-power device issues	Your project extends this by focusing on user-level financial transactions, biometric + picture password authentication, and ZKP verification.

1.4.1 Core Techniques in Threat Detection (Blockchain):

In Abubakar et al. (2023), blockchain was used for intrusion detection by logging network threats securely on a distributed ledger. In contrast, our project (2025), Blockchain Secure Transaction, focuses on user-level transaction protection using Zero-Knowledge Proofs, biometric, and picture password authentication, ensuring privacy and verification before any transaction is approved or blocked.

1.4.2 Blockchain Technology for Proactive and Predictive Defence

While Li & Q. (2025) used blockchain to share intrusion alerts across nodes for proactive defense in network systems, our project (2025) applies blockchain for real-time transaction verification. By integrating ZKP, smart contracts, and biometric authentication, it proactively prevents fraudulent or unauthorized transactions before they occur.

1.4.3 Automated Mitigation and Response(Blockchain Technology):

In the *Blockchain Secure Transaction* system, blockchain enables automated mitigation and response by using smart contracts to instantly detect and react to security breaches or unauthorized transactions. When any irregular activity is identified—such as a failed Zero-Knowledge Proof (ZKP) verification or invalid authentication—the smart contract automatically triggers actions like blocking, freezing, or reversing the transaction.

This eliminates the need for manual intervention and ensures rapid containment of threats. The immutable ledger records every response, allowing transparent audit and future analysis. This automated defence mechanism creates a self-regulating system that maintains integrity, minimizes downtime, and enhances overall transaction security.

1.5 Technical and Accessibility Barriers :

In Zhou et al. (2024), implementing ZKP in blockchain systems faced high computational costs and complex proof generation, limiting real-world deployment. Similarly, our project (2025),

though secure and decentralized, encounters challenges like integration complexity, user accessibility for biometric systems, and ensuring smooth performance across all devices.

1.5.1 Identified Research Gaps :

Existing studies such as Zhang et al. (2024) and Li & Q. (2025) focus on blockchain for data privacy and intrusion detection but lack end-to-end user authentication and transaction-level security.Most research emphasizes network defense or data exchange, while our project (2025) addresses this gap by combining Zero-Knowledge Proofs, biometric and picture password authentication, and smart contracts to ensure secure, verifiable, and user-centric blockchain transactions.

1.5.2 Technical and Accessibility Barriers :

Studies like USENIX (2025) highlight that implementing zk-SNARKs and blockchain-based verification involves high computational requirements and complex setup procedures. Similarly, our project (2025) faces technical barriers such as integrating biometric and picture password authentication with blockchain and ensuring accessibility for all users without compromising transaction speed or system usability.

1.6 Future Scope & Opportunities :

- Expansion to multi-currency and cross-border blockchain transactions for global usability.
- Implementation of quantum-resistant encryption to ensure long-term data protection.
- Development of a mobile-based decentralized application (DApp) for easy user access.
- Integration with banking and government systems for secure digital payments and identity verification.
- Use of advanced biometric methods like facial or voice recognition for improved authentication.
- Addition of real-time transaction tracking dashboards for enhanced transparency.
- Enhancement of smart contract automation for faster and more reliable transaction validation.
- Adoption of cloud–blockchain hybrid systems for better scalability and performance.
- Research on energy-efficient blockchain mechanisms to reduce resource consumption.
- Introduction of user-friendly recovery systems for lost credentials or biometric mismatches.

1.7 Conclusion :

The proposed project, Blockchain Secure Transaction, presents a secure and decentralized framework that ensures privacy, integrity, and transparency in digital transactions. By integrating Zero-Knowledge Proofs (ZKP), biometric verification, and picture password authentication, the system provides multi-layered protection against unauthorized access and data breaches.

The use of smart contracts automates transaction verification, while Firebase integration ensures reliable data storage and retrieval. Unlike traditional centralized systems, this approach eliminates single points of failure and enhances trust among users. Overall, the project demonstrates a practical and scalable solution for secure, tamper-proof, and user-friendly blockchain-based transactions, paving the way for future advancements in decentralized financial systems.

2.0 References :

- Zhang, B., Pan, H., & Li, K. (2024). A Blockchain and Zero-Knowledge Proof Based Data Security Transaction Method in Distributed Computing. MDPI – Electronics.
- Katari, P., Alluri, V. R., & Bojja, S. G. R. (2024). Balancing Openness and Secrecy: ZKP Implementation in Blockchain Transactions. IJISAE Journal.
- Guo, H., Du, X., & Zhang, Y. (2024). Research on Blockchain Smart Contract Application and Security Issues. Journal of Computer Applications & Security.
- Bamashmos, S., Chilamkurti, N., & Shahraki, A. S. (2024). Two-Layered Multi-Factor Authentication Using Decentralized Blockchain in an IoT Environment. MDPI – Sensors.
- Liao, Z., Hao, S., Nan, Y., & Zheng, Z. (2024). SmartState: Detecting State-Reverting Vulnerabilities in Smart Contracts. arXiv / ACM.
- Li, Q., & Zhang, W. (2025). Enhanced Blockchain Collaborative Intrusion Detection System. SpringerLink.
- Wang, Y., & Liu, J. (2024). Decentralized Identity Verification Using Blockchain. ScienceDirect.
- Kumar, R. (2025). Firebase-Integrated Blockchain Transaction Management System. IEEE Xplore.
- Zhou, M., et al. (2024). Leveraging Zero-Knowledge Proofs for Blockchain-Based Identity. ScienceDirect.
- USENIX (2025). Understanding zk-SNARKs: The Gap Between Research and Practice. USENIX Conference Proceedings.