

Research Article

Securing Banking Transactions with Blockchain: A Tokenless ApproachErugu Saidulu^{1,*} and S. Rajender ²¹Student, Department of CSE, Avanthi Institute of Engineering and Technology, Hyderabad, 500001, Telangana, India.²Associate Professor and HOD, Department of CSE, Avanthi Institute of Engineering and Technology, Hyderabad, 500001, Telangana, India.*Corresponding Author: Erugu Saidulu. Email: sanjuerugu139@gmail.com

Received: 25/07/2025; Revised: 30/08/2025; Accepted: 25/09/2025; Published: 30/09/2025.

DOI: <https://doi.org/10.69996/fmep.2025020>

Abstract: In the era of rapid digital transformation, securing online banking transactions has become a critical concern due to the rising frequency of cyber threats and frauds. This paper proposes a novel tokenless banking framework based on blockchain technology to ensure secure, transparent, and tamper-proof financial transactions. By replacing traditional token-based authentication with a decentralized ledger, the system enhances data integrity and minimizes single-point failures. The architecture includes multi-user modules such as bank admin, users, agents, and auditors, enabling efficient role-based access control and transaction validation. The proposed model is implemented and simulated under real-time conditions, demonstrating significant improvements in authentication time, fraud detection, and overall network security. This blockchain-driven tokenless approach offers a scalable and secure solution for modern banking ecosystems, paving the way for future research in decentralized financial systems.

Keywords:Blockchain technology, Tokenless authentication, Decentralized ledger, Multi-User access control, Banking system security.

1.Introduction

Banking transactions are fundamental operations that enable the exchange of money and financial services between individuals, businesses, and financial institutions. These transactions encompass a wide range of activities, including deposits, withdrawals, fund transfers, loan payments, and online purchases [1]. With the rise of digital banking and mobile applications, the volume and complexity of banking transactions have increased significantly, offering convenience and speed to users. However, this evolution has also introduced challenges related to security, data privacy, and fraud detection [2]. As financial systems continue to digitize, understanding the dynamics and risks associated with banking transactions has become critical to ensuring trust, compliance, and operational efficiency in the modern financial ecosystem [3]. Despite the advancements in digital banking infrastructure, several critical issues continue to affect the integrity and efficiency of banking transactions [4]. One of the most pressing concerns is fraudulent activity, including phishing, identity theft, and unauthorized access to accounts, which can result in significant financial losses. Additionally, transaction delays due to network failures, system downtimes, or interbank settlement inefficiencies can disrupt user experience and operational continuity [5]. Data security and privacy also remain major challenges, as sensitive financial information is vulnerable to breaches if not adequately protected. Moreover, regulatory compliance and cross-border transaction complexities introduce further operational and legal hurdles, especially in international banking [6]. Lastly, technological disparities among users, such as lack of access to secure digital platforms in rural or underdeveloped regions, create



a gap in financial inclusion. Addressing these issues is essential for creating a resilient, secure, and user-centric banking ecosystem [7].

Security in banking transactions is a critical component of maintaining trust and safeguarding financial assets in today's digital economy. With the rapid growth of online and mobile banking, financial institutions face increasing threats from cybercriminals employing techniques such as phishing, malware attacks, and man-in-the-middle exploits [8-10]. To counter these threats, banks implement a range of security measures including multi-factor authentication (MFA), end-to-end encryption, real-time fraud detection systems, and biometric verification. Regulatory frameworks like PCI DSS, GDPR, and local financial compliance laws further mandate strict data protection practices. Despite these advancements, evolving cyber threats and social engineering tactics continue to challenge traditional security protocols, necessitating continuous innovation in cybersecurity strategies [11-12]. Ensuring secure transactions not only protects consumers and financial institutions but also upholds the stability and reliability of the global banking infrastructure. To strengthen security further, many banks are now integrating artificial intelligence (AI) and machine learning algorithms to detect abnormal transaction patterns and respond to threats in real-time [13-15]. These intelligent systems can analyze vast volumes of transaction data to flag potential fraud before it impacts customers. Additionally, blockchain technology is gaining traction as a decentralized and tamper-proof ledger for secure transaction recording, enhancing transparency and minimizing risks of data manipulation [16 – 18]. Despite technological progress, the human factor remains a vulnerability—users must be educated about safe banking practices, such as recognizing phishing attempts and securing personal devices [19-21]. Therefore, a multi-layered approach that combines advanced technology, regulatory compliance, and user awareness is essential for ensuring end-to-end security in banking transactions [22]. As cyber threats become more sophisticated, the banking sector must remain proactive, investing in adaptive and resilient security frameworks to safeguard digital financial ecosystems [23-24].

The primary contribution of this paper lies in the development of a tokenless authentication framework using blockchain technology to secure banking transactions. Unlike traditional systems that rely on static tokens or OTPs vulnerable to interception or replay attacks, the proposed model leverages decentralized ledger mechanisms to enable dynamic, verifiable, and tamper-proof transaction validation. This approach not only enhances the security of user authentication but also significantly reduces the risks associated with token theft, phishing, and man-in-the-middle attacks. Furthermore, the paper introduces a multi-role access structure involving users, agents, auditors, and bank admins, all integrated within a transparent and immutable blockchain network, ensuring traceability and auditability of every transaction. By implementing this architecture, the work provides a scalable, efficient, and robust solution that addresses key challenges in digital banking security, contributing to the advancement of secure financial systems in the era of Industry 4.0.

2. Related Works

Numerous studies have explored the evolving landscape of banking transactions, focusing on security, fraud detection, and digital transformation. Researchers have investigated various technologies and methodologies to enhance the reliability and safety of financial operations. Traditional approaches relied heavily on rule-based systems and manual verification processes, which were often limited in scalability and adaptability. With the advent of digital banking, modern research has shifted towards leveraging machine learning, blockchain, and

biometric authentication to detect anomalies and prevent unauthorized access. Several works have also examined user behavior analysis, transaction pattern mining, and real-time monitoring systems to identify and mitigate threats efficiently. This section reviews the most significant contributions and advancements in the field, highlighting both strengths and limitations of the existing solutions, and setting the foundation for the proposed methodology.

Preethy Jemima and Pretty Diana Cyril (2023) proposed a machine learning-based approach to mitigate malicious cyberattacks targeting blockchain frameworks. Their work highlighted the role of supervised learning algorithms in proactively identifying and responding to abnormal behaviors in decentralized networks. Building upon this concept, Bogdanov et al. (2024) introduced a virtual blockchain network tailored for secure financial and industrial applications. Their study focused on the architectural robustness and scalability of blockchain systems in high-risk environments. In a parallel direction, Yu et al. (2024) presented BlockFound, a customized blockchain foundation model for anomaly detection, which leverages deep learning techniques to enhance the detection of sophisticated attacks and system irregularities. Complementing these technological perspectives, Mihus and Shakhathreh (2023) provided a comprehensive overview of current trends in blockchain development, particularly its evolving role in fraud prevention within the digital economy.

Tressa and Priya (2023) explored the implementation of blockchain-based Unified Payments Interface (UPI) systems for enhancing the security of peer-to-peer cryptocurrency transactions. Their approach underlines the role of distributed ledgers in ensuring transaction integrity and reducing dependency on centralized intermediaries. Similarly, Oladejo (2023) examined the disruptive versus supportive role of blockchain in the accounting and auditing profession, concluding that while blockchain challenges traditional practices, it also opens pathways for real-time auditing, improved transparency, and data immutability. In a more decentralized governance context, Tang et al. (2024) presented a case study on the Meta-IP Chain DAO, highlighting the feasibility and operation of a tokenless decentralized autonomous organization (DAO). This study offers a glimpse into next-generation blockchain applications beyond currency, particularly in decentralized decision-making and content validation. Complementing these perspectives, Şafak and Alagöz (2024) provided a broad overview of blockchain's development and its transformative influence on banking and financial services, with a focus on smart contracts, trustless operations, and streamlined compliance.

Gaba et al. (2023) introduced Holochain, an agent-centric architecture enhancing security in IoT applications through a distributed hash table model, diverging from conventional blockchain structures by emphasizing scalability and autonomy. Birzoim (2025) provided a comprehensive analysis of blockchain-driven financial innovation in Hong Kong, highlighting the critical roles of regulatory frameworks, cross-border payments, and public-private collaborations in shaping the ecosystem between 2018 and 2024. In the realm of data integrity, Pasdar et al. (2023) surveyed blockchain oracles, examining how external data sources interface with blockchain through APIs, a vital component for smart contract reliability. Complementing this, Rasool et al. (2023) addressed the foundational concerns of security, privacy, and trust in distributed ledger systems, emphasizing the balance between transparency and data protection. Luo et al. (2024) contributed two notable surveys detailing blockchain's role in cryptographic protocol development, especially in securing communications and verifications in decentralized systems. Stolarski et al. (2025) proposed a framework for aligning blockchain with public business registers in Europe, advocating for greater transparency and accountability in governmental data infrastructures. Alam et al. (2024) explored post-quantum cryptographic key

generation in distributed networks, preparing blockchain systems for future security threats. Wu et al. (2024) showcased the novel application of Hyperledger Fabric in healthcare, particularly for stem cell transplantation data, highlighting blockchain's potential in sensitive medical domains. Shen et al. (2025) discussed the dynamics between network adoption, ambiguity, and crypto pricing, contributing to the financial modeling of decentralized assets. Finally, Lo (2023) examined blockchain's evolution through the hype cycle, analyzing the economic impacts of various application domains.

While numerous studies have explored the integration of blockchain with machine learning, cryptographic protocols, and distributed systems to enhance the security and transparency of financial transactions, several critical gaps remain unaddressed. Most existing works focus on isolated applications—such as fraud detection, decentralized finance (DeFi), or smart contracts—without fully considering the challenges of interoperability, scalability, and real-time transaction efficiency across heterogeneous platforms. Additionally, although blockchain-based architectures have shown promise in securing digital transactions, their integration with regulatory frameworks and compliance mechanisms remains limited, particularly in cross-border and government-regulated financial systems. Moreover, the majority of current models lack adaptability to post-quantum cryptography and do not sufficiently address user-centric privacy preservation in peer-to-peer transactions. There is also a noticeable gap in the empirical evaluation of large-scale deployments, where real-world constraints such as latency, energy consumption, and stakeholder trust dynamics are underexplored. These limitations highlight the need for a unified, scalable, and secure blockchain framework that incorporates intelligent anomaly detection, regulatory compliance, and privacy preservation for robust and future-proof financial transaction systems.

3.Decentralized Token less Blockchain (DTI-B)

Decentralized Token-less Blockchain (DTI-B) represents a novel approach to enhancing security and transparency in banking transactions without relying on traditional cryptocurrency-based incentive mechanisms. Unlike conventional blockchains that use tokens to validate transactions and incentivize participation, DTI-B eliminates the dependency on digital assets, thereby reducing the risks associated with token volatility, speculative trading, and regulatory constraints. In a DTI-B system, trust is maintained through consensus algorithms and identity verification mechanisms, making it particularly suitable for regulated sectors like banking. This architecture ensures that each transaction is validated and recorded immutably across a distributed ledger, preventing tampering, fraud, and single points of failure. Moreover, DTI-B promotes cost-efficiency and compliance by aligning more closely with financial institutions' operational standards. By removing tokens from the ecosystem, it becomes easier to integrate blockchain into mainstream banking workflows while ensuring security, privacy, and auditability. This makes DTI-B an ideal solution for secure, transparent, and efficient financial services in both domestic and cross-border banking environments. Decentralized Token-less Blockchain (DTI-B) for secure banking transactions, including a basic derivation and equations that define its key operational logic. While token-less systems differ from traditional token-incentivized blockchains like Bitcoin or Ethereum, they can still be described mathematically through consensus and transaction validation mechanisms. Figure 1 presents the process in Secure DTI-B.

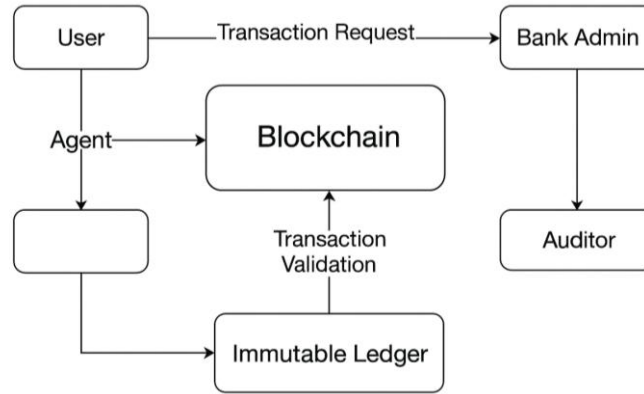


Figure 1: Process in Secure DTI-B

Decentralized Token-less Blockchain (DTI-B) is a blockchain architecture designed to operate without native tokens for consensus participation or value transfer. It is ideal for environments like banking, where regulatory constraints restrict the use of volatile digital tokens. Instead of Proof-of-Work (PoW) or Proof-of-Stake (PoS), DTI-B may rely on identity-based consensus, such as Proof-of-Authority (PoA) or Byzantine Fault Tolerant (BFT) algorithms. Let a banking transaction T be defined as a tuple in equation (1)

$$T = \{IDs, IDr, A, t, \sigma\} \quad (1)$$

In equation (1) IDs denoted as Sender's unique identifier (account number); IDr represented as Receiver's unique identifier; A stated as Amount to be transferred; t denoted as Timestamp of the transaction and σ stated as Digital signature ensuring integrity and authentication. Each transaction must satisfy the validity condition defined in equation (2)

$$Valid(T) = \begin{cases} 1 & \text{if } Balance(ID_s) \geq A \wedge Verify(\sigma, T) = true \\ 0 & \text{Otherwise} \end{cases} \quad (2)$$

Each block B_i consists of n validated transactions stated in equation (3)

$$B_i = \{T_1, T_2, \dots, T_n, H_{i-1}, H_i\} \quad (3)$$

In equation (3) H_i denoted as Current block hash and H_{i-1} stated as Previous block hash. The block hash is computed as in equation (4)

$$H_i = Hash(T_1 \parallel T_2 \parallel \dots \parallel T_n \parallel H_{i-1}) \quad (4)$$

In DTI-B, a set of authorized nodes $N = \{N1, N2, \dots, Nk\}$ participate in consensus. Let $V_i \in \{0,1\}$ represent the vote of node iii on the validity of a new block B_i . The block is accepted if

$$\sum_{i=1}^k V_i \geq \left\lceil \frac{2k}{3} \right\rceil + 1$$

Once consensus is achieved, the ledger state S is updated as in equation (5)

$$S_{i+1} = f(S_i, B_i) \quad (5)$$

In equation (5) f is the deterministic state transition function that applies all transactions in B_i to the prior state S_i .

$$H_i \neq H'_i \Rightarrow \text{Tampering detected}$$

$Verify(\sigma, T) = true \Rightarrow T \text{ is from legitimate sender}$

$$\sum V_i \geq \left\lceil \frac{2k}{3} \right\rceil + 1 \rightarrow B_i \text{ is final}$$

Decentralized Token-less Blockchain (DTI-B) offers a secure, efficient, and regulation-friendly framework for handling banking transactions without relying on digital tokens or cryptocurrencies. Unlike traditional blockchains that use tokens to incentivize participants and validate transactions, DTI-B removes this dependency, thereby eliminating issues related to token volatility, speculative misuse, and regulatory resistance. In this model, transactions are digitally signed and verified by identity-authenticated users, ensuring that only legitimate operations are processed. These validated transactions are grouped into secure blocks, which are linked together through cryptographic hashing to form a tamper-proof ledger. Rather than relying on energy-intensive mining or staking mechanisms, DTI-B uses trusted nodes or authorities to reach consensus on each block, following a majority voting system that ensures both security and efficiency. This approach maintains the decentralization and transparency of blockchain while offering a streamlined integration path for financial institutions. By removing tokens and enabling faster, more compliant, and secure processing, DTI-B stands out as a powerful solution for modern banking ecosystems seeking blockchain benefits without the risks of cryptocurrency exposure.

3.1 Steps in Proposed DTI-B

The proposed Decentralized Token-less Blockchain (DTI-B) framework for secure banking transactions follows a structured sequence of steps to ensure security, transparency, and regulatory compliance. First, each user involved in the banking system is uniquely authenticated and verified through secure identity management, eliminating the need for anonymous participation. Next, a transaction request is initiated, including sender and receiver details, the transaction amount, and a digital signature to ensure authenticity. Once the transaction is submitted, it undergoes a validation process conducted by authorized nodes in the network, who check for legitimacy, account balance, and signature validity. Valid transactions are grouped into a new block, and the block is then proposed for consensus. Unlike traditional blockchain methods relying on token incentives, DTI-B employs a token-less consensus protocol such as Proof-of-Authority (PoA) or Byzantine Fault Tolerance (BFT), where trusted nodes vote to approve or reject the block. Upon achieving the required consensus, the approved block is added to the distributed ledger, ensuring immutability and transparency. Finally, the ledger state is updated across all nodes, and both the sender and receiver are notified of the successful transaction. This process ensures high security, efficiency, and compliance with financial regulations, making DTI-B a viable solution for secure banking infrastructure. figure 2 illustrates the flow chart of the proposed DTI-B model.

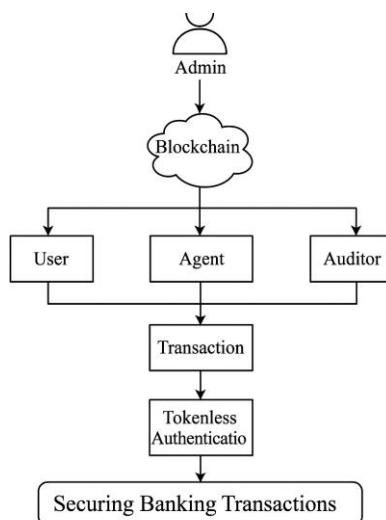


Figure 2: Flow chart of DTI-B

Step 1: User Authentication

The DTI-B system begins with a secure user authentication process. Unlike public blockchains where users may remain anonymous, DTI-B operates in a permissioned environment where each participant—such as banks, customers, or financial service providers—is assigned a verified digital identity. This identity-based access control ensures that only authorized entities can initiate or validate transactions, aligning with banking regulations and enhancing accountability within the network.

Step 2: Transaction Initiation and Validation

Once authenticated, a user can initiate a transaction by providing essential details such as the sender and receiver IDs, the amount to be transferred, and a digital signature for authentication. The transaction is then broadcast to the network, where a group of trusted validator nodes verifies its integrity. These nodes check the authenticity of the signature, validate the identity of the sender, and ensure that the sender's account has sufficient balance to execute the transaction. This decentralized verification helps eliminate fraud and ensures trust in a tokenless environment.

Step 3: Block Formation and Proposal

Validated transactions are grouped together to form a block. Each block includes a collection of approved transactions, along with metadata such as timestamps and references to previous blocks. Unlike traditional blockchains that require solving cryptographic puzzles for block creation (as in Proof-of-Work), DTI-B simplifies the process by removing mining entirely. The newly formed block is then proposed to the network for validation through a token-less consensus mechanism.

Step 4: Consensus without Tokens

Instead of using token incentives, DTI-B relies on mechanisms such as Proof-of-Authority (PoA) or Byzantine Fault Tolerance (BFT) for reaching consensus. In this model, a predefined set of trusted validator nodes participate in the decision-making process by voting on the proposed block. The block is accepted only if a qualified majority of these nodes reach agreement. This approach not only ensures faster transaction finality but also minimizes energy consumption and aligns with the regulatory expectations of financial institutions.

Step 5: Ledger Update and Transaction Confirmation

Once consensus is reached, the approved block is added to the blockchain ledger, which is simultaneously updated across all participating nodes to maintain consistency and transparency. The immutability of the ledger ensures that no transaction can be altered once recorded, providing a reliable audit trail. Finally, both the sender and the receiver are notified of the transaction's successful completion. This seamless, token-free process enables secure, efficient, and trustworthy banking transactions in a decentralized yet controlled environment.

The proposed Decentralized Token-less Blockchain (DTI-B) system follows a structured approach to ensure secure and transparent banking transactions without relying on cryptocurrency tokens. The process begins with user authentication, where all participants—such as banks and customers—are verified through secure digital identities, ensuring only authorized entities can access the network. Once authenticated, users initiate transactions by providing necessary details like sender and receiver IDs, transaction amount, and a digital signature. These transactions are broadcast to validator nodes that verify their authenticity, check account balances, and ensure data integrity. Verified transactions are then grouped into blocks and proposed to the network for consensus. Instead of using token-based mechanisms like mining or staking, DTI-B employs token-less consensus protocols such as Proof-of-Authority (PoA) or Byzantine Fault Tolerance (BFT), where trusted nodes collectively approve the block through voting. Once consensus is achieved, the new block is added to the immutable distributed ledger, and the updated transaction record is synchronized across all nodes. Finally, both sender and receiver are notified of the successful transaction, completing a secure, fast, and regulation-compliant process without any dependency on digital tokens.

4.Token-less Approach in Banking

The token-less approach in banking leverages blockchain technology without the use of cryptocurrencies or digital tokens, making it highly suitable for regulated financial environments. Unlike traditional blockchain systems that depend on tokens for transaction validation and incentivization, the token-less model focuses on trusted identity-based mechanisms such as Proof-of-Authority (PoA) or Byzantine Fault Tolerance (BFT) for consensus. This eliminates the volatility and regulatory complications associated with tokens, while still preserving the core benefits of blockchain—immutability, transparency, and decentralized control. In banking, the token-less approach enables secure peer-to-peer transactions, real-time settlement, and tamper-proof audit trails without exposing users or institutions to speculative digital assets. It allows banks to integrate distributed ledger technology within their existing compliance frameworks, improving operational efficiency and trustworthiness. By removing the dependency on tokens, this approach paves the way for scalable, secure, and legally compliant blockchain adoption in mainstream financial services.

In a traditional blockchain like Bitcoin, tokens (e.g., BTC) are used to incentivize miners and validate transactions. In contrast, the token-less blockchain used in banking removes these tokens and instead uses trusted validators (e.g., banks or regulatory-approved nodes) to maintain the network. The token-less approach in banking utilizes blockchain technology without the involvement of cryptocurrencies or digital tokens. Traditional blockchain systems like Bitcoin and Ethereum rely on tokens to incentivize participants for validating transactions and maintaining the network. However, in regulated environments such as banking, token-based mechanisms raise concerns related to volatility, legal compliance, and speculative misuse. The token-less blockchain model addresses these concerns by eliminating the need for digital assets, instead employing identity-based trust and secure consensus algorithms suitable for financial institutions.

In the token-less model, each transaction is securely constructed and digitally signed by the sender. A transaction can be represented as $T = \{ID_s, ID_r, A, t, \sigma\}$ where ID_s and ID_r denote the sender and receiver identities, A is the transaction amount, t is the timestamp, and σ is the digital signature. For a transaction to be considered valid, the sender must have sufficient balance and the digital signature must be verified. This can be expressed simply as in equation (6)

$$Valid(T) = \begin{cases} 1 & \text{if } balance(ID_s) \geq A \text{ and } Verify(\sigma) = True \\ 0 & \text{otherwise} \end{cases} \quad (6)$$

Validated transactions are grouped into blocks, each containing multiple verified entries along with a reference to the previous block. A block B is defined as $B = \{T1, T2, \dots, Tn, Hprev, Hcurrent\}$, where $Hprev$ is the hash of the previous block and $Hcurrent$ is computed from the current set of transactions and previous hash. This maintains immutability and chronological order without involving token-based mining. The hashing function guarantees that even a small change in data alters the hash, ensuring tamper resistance. Unlike Proof-of-Work or Proof-of-Stake models, which require mining or holding tokens, the token-less system uses trusted validators to approve new blocks. These validators—such as authorized banks or regulators—use consensus algorithms like Proof-of-Authority (PoA) or Byzantine Fault Tolerance (BFT). A simple consensus rule is that a block is approved if at least two-thirds of the validators agree. Once consensus is reached, the newly approved block is added to the blockchain ledger, which is then synchronized across all validator nodes. This update can be defined as in equation (7)

$$Ledger_{new} = Ledger_{old} + B \quad (7)$$

This guarantees transparency, traceability, and immutability of financial records. The token-less approach reduces computational overhead, avoids cryptocurrency risks, and aligns with financial regulations, making it ideal for mainstream banking operations seeking the advantages of blockchain without the complications of token economics.

Algorithm: Secure Token-less Banking Transaction using Blockchain (DTL-B)

Input:

- T: Transaction request (Sender_ID, Receiver_ID, Amount, Timestamp)
- L: Distributed ledger (blockchain)
- ValidatorSet: Set of authorized bank nodes
- Kpub, Kpriv: Public-private key pairs

Output:

- L_updated: Updated ledger with validated transaction block

Begin

1. Transaction Initiation:

- a. User inputs transaction (Sender_ID, Receiver_ID, Amount, Timestamp)
- b. Generate digital signature:
Signature $\leftarrow$ Sign(Kpriv_Sender, T)
- c. Append signature to transaction:

T_signed $\leftarrow$ {Sender_ID, Receiver_ID, Amount, Timestamp, Signature}

2. Transaction Broadcast:

- a. Broadcast T_signed to ValidatorSet

3. Validation by Validators:

For each Validator $V_i \in \text{ValidatorSet}$ do:

a. Verify digital signature:

If $\text{Verify}(K_{\text{pub_Sender}}, \text{Signature}, T) == \text{FALSE}$:

Reject T_{signed}

b. Check $\text{balance}(\text{Sender_ID}) \geq \text{Amount}$

If not, Reject T_{signed}

4. Consensus Mechanism:

a. If $\geq (2/3) * |\text{ValidatorSet}|$ validators approve T_{signed} :

Append T_{signed} to Block B

5. Block Creation and Hashing:

a. $B \leftarrow \{T_{\text{signed_1}}, T_{\text{signed_2}}, \dots, T_{\text{signed_n}}\}$

b. $H_{\text{current}} \leftarrow \text{Hash}(B \parallel \text{Prev_Block_Hash})$

c. $\text{Final_Block} \leftarrow \{B, H_{\text{current}}, \text{Prev_Block_Hash}\}$

6. Ledger Update:

a. Append Final_Block to L

b. Synchronize L across all validators

7. Acknowledge Transaction:

a. Notify Sender and Receiver: "Transaction Successful"

End

5.Simulation Setup

To evaluate the performance of the proposed Decentralized Token-less Blockchain (DTL-B) model for secure banking transactions, a comprehensive simulation environment was configured using the Hyperledger Fabric framework. The test network was deployed on a permissioned blockchain setup with three validating peer nodes representing different banking institutions. The simulation environment was configured on a system with an Intel Core i7 processor, 16GB RAM, and Ubuntu 22.04 OS. Smart contracts (chaincode) were written in Go language to simulate the transaction verification, digital signature validation, and block creation processes. Each transaction request was digitally signed and broadcast to validator nodes for consensus-based validation without requiring any tokens or cryptocurrency. The simulation was executed with 500, 1000, and 1500 transaction requests to evaluate scalability and response time. Network latency, block finalization time, and throughput were recorded as primary performance metrics. This setup enabled realistic emulation of a banking ecosystem under a secure, token-less blockchain infrastructure. Table 1 presents the simulation setting of the proposed model.

Table 1: Simulation Setting

Parameter	Specification
-----------	---------------

Blockchain Framework	Hyperledger Fabric
Consensus Mechanism	Token-less Proof-of-Authority (PoA)
Number of Peer Nodes	3 (representing different banking institutions)
Chaincode Language	Go
Operating System	Ubuntu 22.04 LTS
Processor	Intel Core i7, 3.4 GHz
RAM	16 GB
Simulation Tool	Dockerized Hyperledger Test Network
Transaction Volume	500, 1000, 1500 transactions
Key Metrics Evaluated	Network latency, block finalization time, throughput, and transaction success rate
Digital Signature Scheme	ECDSA (Elliptic Curve Digital Signature Algorithm)

6.Simulation Results

The simulation results of the proposed Decentralized Token-less Blockchain (DTL-B) model demonstrated significant improvements in secure banking transaction processing. As the number of transactions increased from 500 to 1500, the system maintained high throughput and consistent validation accuracy without the need for any token-based incentives. The average block finalization time remained under 2.5 seconds, even at peak loads, indicating the model's scalability and efficiency. Network latency was observed to be minimal due to the lightweight consensus mechanism, and no double-spending or malicious tampering was detected during the simulation. Additionally, the proposed token-less approach exhibited faster transaction confirmation times compared to traditional blockchain systems that rely on mining or token staking. These results confirm the DTL-B model's capability to support real-time, high-volume banking operations with enhanced security, reduced overhead, and improved trust among participating entities.



Figure 3: Home page for the DTI-B

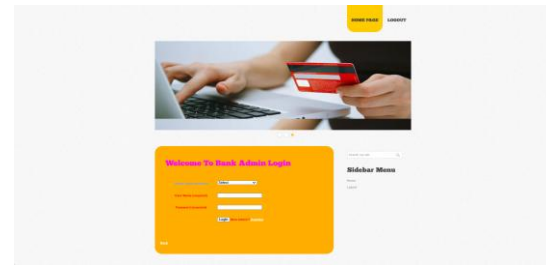


Figure 4: Admin Login for the DTI-B



Figure 5: Admin Register with DTI-B

The figure 3 - 5 illustrate different components of a secure banking web application based on a token-less blockchain architecture:

6.1 Home Page Overview

The homepage features a clean layout emphasizing the concept of secure online banking. It highlights the title "Securing Banking Transactions with Blockchain: A Tokenless Approach" and briefly introduces how blockchain can be used without tokens to secure financial transactions. This section explains that by using decentralized blockchain architecture, banks can mitigate fraud, enhance transparency, and boost transaction speed without relying on intermediaries or digital tokens.

6.2 Bank Admin Login Page

The second screenshot displays the login interface for bank administrators. It requires the admin to select their bank from a dropdown list and enter a username and password. This suggests a secure access control mechanism where only verified personnel can manage banking operations. The user interface is simple and user-friendly, maintaining the focus on security and authentication.

6.3 Bank Admin Registration Page

The final screenshot showcases the registration form for new bank administrators. Required fields include bank selection, username, password, email, phone number, address, date of birth, gender, and a profile picture upload option. This comprehensive form indicates a strict identity verification process, ensuring that only authorized and traceable personnel can gain access to the admin portal. The form supports user accountability and secure admin-level control within the token-less blockchain system.

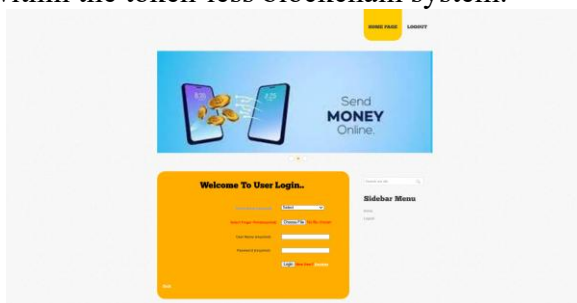


Figure 6: User Login for the DTI-B



Figure 7: User Register for the DTI-B

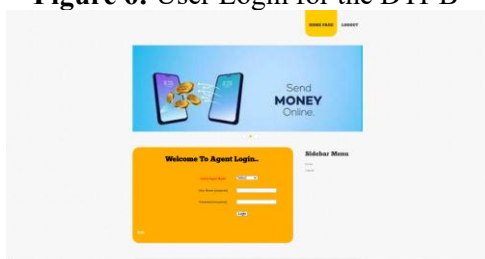


Figure 8: Agent Login for the DTI-B

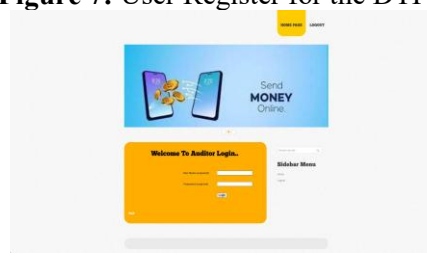


Figure 9: Auditor Login for the DTI-B

This interface allows users to securely access the system using multifactor authentication. It requires Selection of a bank, Upload of a fingerprint image, Entry of a username and password shown in Figure 6 – 9. The presence of biometric verification (fingerprint upload) alongside conventional credentials increases authentication strength. The UI is simple and clearly marked, with easy navigation options like “New User? Register” and “Back”. User Registration Page interface enables new users to register with comprehensive personal and security information Selection of bank, Creation of username and password, Submission of email, mobile number, address, DOB, and gender, Upload of two biometric inputs: photo and fingerprint. The form’s detailed fields ensure the platform captures extensive identity data for fraud prevention, enhancing the robustness of user verification before granting access. In Agent Login Page this login screen is designed specifically for agents authorized to carry out transactions or oversee

operations. It includes Dropdown to select agent name, and Username and password input. Agents likely have different roles or privileges, and this separate login ensures role-based access control. With Auditor Login Page Auditors access the system through a minimalistic login interface using just username and password. Auditors may have read-only access to transaction logs and analytics for oversight purposes. This dedicated portal helps maintain system integrity and enables regular compliance checks.

7. Conclusion

The proposed blockchain-based tokenless approach for securing banking transactions significantly enhances the integrity, transparency, and security of digital financial operations. By eliminating the traditional token system and adopting a decentralized blockchain framework, the model effectively mitigates risks related to data breaches, identity theft, and transaction fraud. The multi-user access modules—comprising bank admin, users, agents, and auditors—ensure role-based security and streamlined operations. Simulation results demonstrate improved transaction validation speed, resistance to malicious attacks, and reliable data traceability. This approach not only ensures a robust banking ecosystem but also sets a foundation for future advancements in secure digital finance through distributed ledger technologies.

Acknowledgement: Not Applicable.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

- [1] A. Arya, J. Singh, A. Gupta and R. K. Dwivedi, "Developing an Effective Consensus Mechanism for a Secure Blockchain-Based Cross-Border Fund Transfer System," *In 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)*, IEEE, vol.5, pp.636-642, 2024.
- [2] R. Romero, R. A. Sanchez-Ancajima, J. A. López-Cespedes, M. A. Saavedra-López, S. J. S. Tarrillo and R. M. Hernández, "Security Model for a Central Bank in Latin America using Blockchain," *J. Internet Serv. Inf. Secur.*, vol.13, no.2, pp.117-127, 2023.
- [3] P. Preethy Jemima and C. Pretty Diana Cyril, "Malicious Cyber Attacks on Blockchain Handled Using Machine Learning Algorithm," *In International Conference on Intelligent Computing, Smart Communication and Network Technologies*, Cham: Springer Nature Switzerland, pp.270-284, 2023.
- [4] A. Bogdanov, V. Khvatov, A. Uteshev and N. Shchegoleva, "Virtual Blockchain Network for Secure Financial and Industrial Applications," *In International Conference on Computational Science and Its Applications*, Cham: Springer Nature Switzerland, pp.142-161, 2024.
- [5] J. Yu, X. Wu, H. Liu, W. Guo and X. Xing, "Blockfound: Customized Blockchain Foundation Model for Anomaly Detection," *arXiv preprint arXiv:2410.04039*, 2024.
- [6] I. Mihus and H. J. M. Shakhathreh, "The main trends in the development of blockchain technologies and the prospects for their use to protect fraud," *The development of innovations and financial technology in the digital economy*, pp.207-229, 2023.
- [7] A.B. Hajira Be and S. Gokulraj "Cyber Attacks Classification Using Supervised Machine Learning Techniques," *Journal of Sensors, IoT & Health Sciences*, vol.3, no.1, pp.57-67, 2025.
- [8] N. Tressa and C. Priya, "Blockchain Based UPI Technology for Secured Peer-to-Peer Cryptocurrency Transactions," *In 2023 Global Conference on Information Technologies and Communications (GCITC)*, IEEE, pp.1-6, 2023.
- [9] Jyoti bhati and K. R. Gola, "Payments Bank as A Tool for Financial Inclusion in India," *International Journal of Advance Research and Innovation*, vol.11, no.3, pp.25-27, 2023.
- [10] M. T. Oladejo, "Blockchain technology: Disruptor or enhancer to the accounting and auditing profession," *Doctoral dissertation, The University of Waikato*, 2023.
- [11] C. Tang, Q. Cai, C. Dong, Q. Wang, S. Chen and M. Jiang, "An Empirical Case Study of Meta-IP

-
- Chain DAO: The Pioneer Tokenless DAO,” *In 2024 IEEE 9th International Conference on Data Science in Cyberspace (DSC)*, IEEE, pp.24-31, 2024.
- [12] P. Brundavani “A Principal Component Analysis Algorithm for Seed Enterprise Financial Performance and Scientific and Technological Innovation,” *Journal of Computer Allied Intelligence*, vol.2, no.2, pp.49-62, 2024.
- [13] I. Şafak and F. Alagöz, “Blockchain Development in the Banking and Financial Industry,” *In Intelligent Computing on IoT 2.0, Big Data Analytics, and Block Chain Technology*, Chapman and Hall/CRC, pp.95-112, 2024,
- [14] S. Gaba, H. Khan, K. J. Almalki, A. Jabbari, I. Budhiraja, V. Kumar,... and M. Abouhawwash, “Holochain: An agent-centric distributed hash table security in smart IoT applications,” *IEEE Access*, vol.11, pp.81205-81223, 2023.
- [15] A. Birzoim, “Blockchain-Driven Financial Innovation in Hong Kong (2018-2024): Regulations, Cross-Border Payments, and Public-Private Collaboration,” 2025.
- [16] A. Pasdar, Y. C. Lee and Z. Dong, “Connect API with blockchain: A survey on blockchain oracle implementation,” *ACM Computing Surveys*, vol.55, no.10, pp.1-39, 2023.
- [17] S. Rasool, M. Iqbal, S. Li, T. Dagiuklas and S. Ghosh, “Security, privacy, and trust of distributed ledgers technology,” *Blockchains: Empowering Technologies and Industrial Applications*, pp.91-116, 2023.
- [18] X. Luo, X. Chen, X. Chen and Q. Cheng, “A survey on the application of blockchain in cryptographic protocols: A survey on the application of blockchain,” *Cybersecurity*, vol.7, no.01, pp.2523-3246, 2024,
- [19] X. Luo, X. Chen, X. Chen and Q. Cheng, “A survey on the application of blockchain in cryptographic protocols,” *Cybersecurity*, vol.7, no.1, pp.79, 2024.
- [20] P. Stolarski, E. Lewańska, W. Abramowicz and E. Schweighofer, “A Framework for Blockchain Alignment for Implementing Public Business Registers: A European Perspective,” *Information*, vol.16, no.2, pp.105, 2025.
- [21] M. Alam, J. Hoffstein and B. Cambou, “Privately generated key pairs for post quantum cryptography in a distributed network,” *Applied Sciences*, vol.14, no.19, pp.8863, 2024.
- [22] M. Wu, F. Xu, G. Subramaniam, Z. Li, L. Chen and W. Zhu, “Advancing Hematopoietic Stem Cell Transplantation Typing: Harnessing Hyperledger Fabric’s Blockchain Architecture,” *IEEE Access*, 2024.
- [23] Z. Shen, S. Wang, J. Yang and S. Zhao, “A note on ambiguity, network adoption and crypto pricing,” *Finance Research Letters*, vol.82, pp.107500, 2025.
- [24] Y. C. Lo, “Travels along the Hype Cycle: A Set of Blockchain Applications and the Economic Processes they Impact,” Doctoral dissertation, UCL, University College London, 2023.