International Journal of Information Technology & Computer Engineering

ISSN 2347–3657
Volume 14, Issue 1, 2026

Secure Bank Transaction System Using Blockchain Technology

Sharmila Ramasundaram Sudharsanam[1], Mrs. D.K. Kalai Vani[2]

[1]Department of Computer Science and Engineering, Udaya School of Engineering, Kanyakumari, Tamilnadu, India-629204.
E-Mail-ID: sharmypo@gmail.com

[2]Department of Computer Science and Engineering, Udaya School of Engineering, Kanyakumari, Tamilnadu, India-629204.
E-Mail-ID: dkkalai2011@gmail.com

Abstract
Banking functions require stable and safe systems of online transactions. The goal of the present study is to create a banking system based on block-chain and guaranteeing transparency, immutability, and absence of fraudulent activities. The uniqueness of the presented research thesis is the SBTE design that uses automation of smart contracts with the Ethereum blockchain validation to manage essentially banking operations such as registration, transfer of funds, accounts maintenance, etc. The recommended structure performs authentic transactions and documenting them on the blockchain which are verified by miners to ensure trust and traceability. Findings indicate that there are high proficiency, immediate updated records and proper upkeep of ledgers and in general. Ultimately, SBTE framework will be a very positive and stable banking system that allows running various transactions without interruption and will guarantee transparency and reliability to its users and administrators.

Keywords—*Blockchain, Ethereum, Smart Contracts, Secure Banking, Decentralized Transactions, SBTE, Transaction Accuracy.*

I. Introduction

Digitizing banking on the global scale is a quickly growing trend due to the reason of more efficient use of speed, convenience, and security in banking [1]. Nevertheless, this change has increased the issue of the safety of transactions, their integrity, and fraud prevention. The conventional banking is designed such that the banking system operates on centralized platforms upon which one dominating body dictates the banking system and responsibility of managing ledgers [2]. Although this centralization has the advantage of facilitating a simple operation, there are more vulnerabilities through centralization such as the chance of insider fraud, manipulation, and overall system malfunction because of cyberattacks or technical hindrances [3]. In addition, central models are not always transparent to the customers, and they have to merely follow suit by blindly believing in the institution without the capacity to confirm records on their own. This creates a serious need to find new solutions that would involve transparency, efficiency and high security [4]. A novel technology called blockchain has a significant potential to disrupt the conventional models by bringing a new decentralized model, distributed trust and unchangeable accountability sheets. Contrary to centralized systems, blockchain is a peer-to-peer network in form where all transactions are confirmed through the mechanism of consensus and/or they are written in blocks that cannot be changed [5]. This is to the fact that there would be no single person in charge of the records and data manipulation, ensuring that fraud is greatly reduced [6]. Ethereum has become one of the strongest blockchain discovered among all of them because it supports smart contracts in the form of Turing machines. Such programmable contracts can be used to run an automated, verifiable, and transparent back-end to the banking operations of deposits and withdrawals and transfers without actually having a third party involved [7]. With Ethereum around, the evolution of successful DeFi shows that publicizing secure and large-scale financial transactions is achievable [8]. In this regard, this study develops and analyses the SBTE (Secure Banking on Ethereum), structure that uses the blockchain-based Ethereum platform to build a safe, open, and decentralized banking system. With the help of cryptographic protection and automation of the use of smart contracts, SBTE is supposed to prevent the fraud and boost their customers confidence as well as leave an audit trail of all the transactions. The key contribution of this study followed as below:

- The analysis suggests SBTE, a blockchain infrastructure of a secure and decentralized transaction in banks.
- It establishes intelligent contracts which automate embedded banking services like deposits, withdrawals and fund transfers.
- The system provides the ledger of seed records on the immutable Ethereum ledger and consensus also ensures the tamper-proof, transparent, and audits post.
- It measures it on security, performance, and cost-efficiency, indicating that the framework is practical in the modern banking applications.

The rest of the manuscript is organized in the following manner: Section 2 entails the literature review, Section 3 is the research and methods, Section 4 is the description of the dataset and framework analysis, and Section 5 is the discussion of findings and future work.

II. Literature Review

The use of a blockchain technology application in finance services has become particularly popular these days, in the form of an Ethereum smart contract that offers an opportunity to safer and more automated banking processes. Some works also highlight the practical examples of usage that test the possibilities of blockchain to transform the banking transactions. One

article described using Ethereum smart contracts to enable payment transactions and how programmable contracts can instantiate financial execution and how it can better secure transactions in addition to determining risks through programming weaknesses in Solidity code [9]. In another work, the authors introduced the design of a loan system based on smart contracts without intermediaries any more, storing loan settlements in blockchain code and thereby enhancing trust and eliminating operational delays [10]. Moreover, the works on blockchain-enhanced online banking provided a paradigm of secure authentication and trust management of online financial systems with a strong accent on the possibility of blockchain to offer solid identity check and transparency in conducting transactions [11]. However, the same authors also found the design of smart algorithms designed to allow to minimize the costs of gas usage, and prevent privacy loss by optimizing the design of contracts thus demonstrating that off-chain data management may reduce costs, without sacrificing social efficiency of the system [12]. More recently, a case study of the decentralized applications made the point of integrating wallet security as well as exposing false points of vulnerability, including integer overflow and reentrancy, as critical to blockchain-based financial systems [13]. Regardless of these encouraging tendencies, constraints exist in the literature. Most of the firms are simply undertaking the tests to pilot or experiment with net-based environments and there is little assurance of its functionality in real banking situations. Another problem is scalability, as Ethereum has a worse throughput and latency than the conventional systems [14]. Gas fees contribute to unaffordability and that might not allow users to create microtermediate usage. In addition to it, blockchain has turned out to be transparent and it is linked to privacy issues since the information of the transaction can be viewed on a publicly available ledger [15]. All these restrictions imply that, although Ethereum smart contracts present a valid system of secure and decentralized banking systems, more must be done on the topic of scalability, privacy, and cost effectiveness to implement smart contracts at large scale application.

III. Research Methodology

The study relies on the multi-layered hybrid security architecture HBM-Secure (Hybrid Blockchain-Machine Learning Secure Framework) that may be deployed to offer integrity, confidentiality, and real-time fraud detection to blockchain-based banking systems. Unlike the conventional frameworks, which deduce the focus on the cryptographic power or anomaly detection, HBM-Secure integrates the latest cryptographic primitives, blockchain validation, and machine learning into one framework. It begins with cryptographic security with the help of SHA-3 and bcrypt to guarantee the safety of transactions and passwords and finishes with blockchain verification to guarantee the impossibility of modifying and the possibility of tracking the records. One of the weaknesses of a static rule-based monitoring is a Rand Forest-based anomaly detection system that has been added to overcome its shortcomings. Finally, the framework is analyzed in terms of performance in cryptographic efficiency, fraud detection accuracy and system-level throughput, which makes HBM-Secure a powerful and scalable framework of digital secure transactions. Fig 1 shows the work flow of the study.

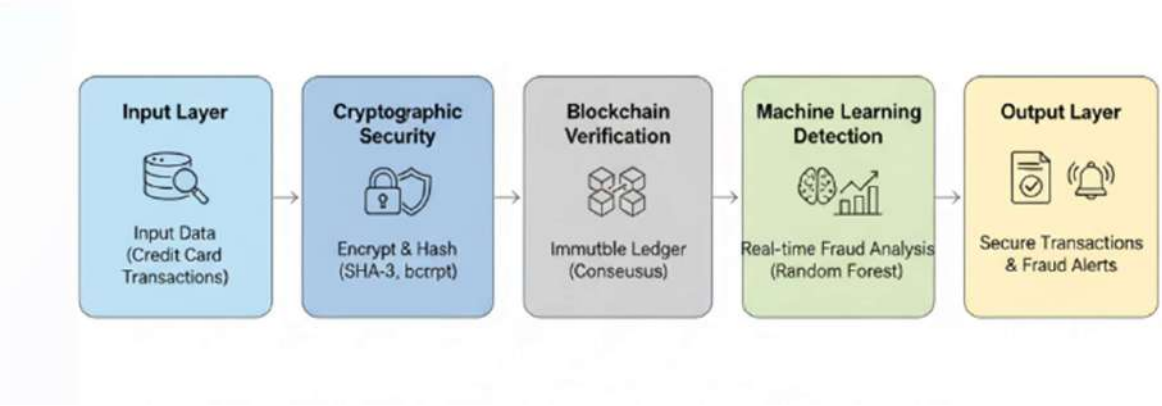

Fig.1. Overall Research Methodology

A. Data Collection

This data would be most appropriate in evaluating the HBM-Secure framework [16], as it would provide a real-world case of asymmetric financial transactions, which would be necessary to gauge the effectiveness of the combative elements of cryptography and machine learning. The anonymity of the data is suitable to the privacy of the blockchain systems, and the fraudulent transactions allow an assessment of the ability of the Random Forest model to identify anomalies within the framework.

B. Cryptographic Security Layer

An integrity of transactions and user authentication in this layer is carried out through cryptographic means. Hashing of any transaction records is performed using the SHA-3 (Keccak) hash algorithm that has better

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 1, 2026

preimage and collision resistance compared to the previous versions of SHA. This will ensure that when a transaction is recorded, it is not able to be altered, or forged and remains flawless within the system. Bcrypt is implemented as a secure hashing mechanism of the key and password in order to secure on an account level. Unlike the situation with the static hashing, the cost factors in bcrypt are dynamic and therefore make brute-force and rainbow table assaults computationally intensive; thereby boosting the security of authentication. The combination of these cryptographic measures offers a strong framework of data confidentiality and integrity in the proposed framework.

C. Blockchain Verification Layer.

The cryptographic hashes are sustained in a permissioned or private blockchain ledger because the blockchain authentication layer improves the safety of the transactions. The chain blocks are all hashed with the help of SHA-3 and provide a tamper-proof storage. The consensus mechanism will verify and confirm the transactions to all the nodes in the network, eliminating the possibility of unauthorized change or spending the same money. This layer is not only immutable but traceable also and the transactions are more transparent since they can be individually verified. The cryptography results are inserted into the blockchain in the framework to provide an uncorruptible audit trail to ensure the safe banking functions.

D. Machine Learning Layer of Anomaly Detection.

This layer offers active monitoring with machine learning to supplement the natural statistic security of the cryptography and blockchain. A Random Forest classifier is calculated by using previous transaction history to obtain the trend of normal and abnormal behaviour. Its learning in the form of an ensemble makes it more accurate to classify and less prone to overfitting. Logistic Regression and Support Vector Machine (SVM) models are also tested to compare the comparative strength in the detection of fraud to benchmark. Any real-time transaction is passed through the trained model to show the presence of abnormalities and thus the system can be able to detect suspicious transactions even before the damage is caused in the financial sector. This predictive nature transforms the structure to a type of active security model, as opposed to a passive operational framework by an intelligent system to thwart fraud.This workflow makes the banking operations auditable, transparent and instilled with confidence by having everything captured in an interim way. Moreover, there is the automation aspect based on smart contracts that eliminates the use of centralized clients thus enhancing efficiency and safety. A general work flow of the research methodology is shown in Fig 2.

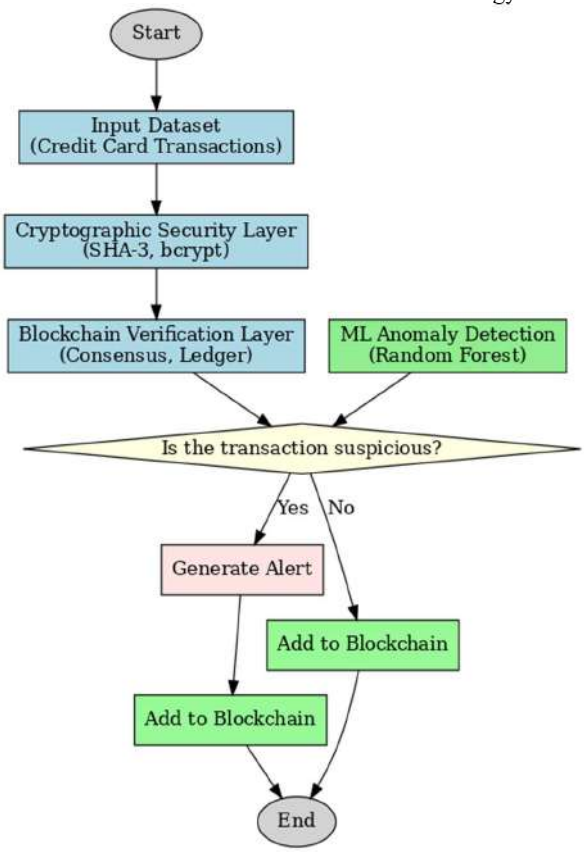

Fig.2. HBM-Secure (Hybrid Blockchain-Machine Learning Secure Framework)

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 1, 2026

Algorithm 1 is demonstrates the overall research methodology of the study.

Algorithm 1: HBM-Secure Algorithm

Input:
T_train ← Historical transaction dataset
T_stream ← Incoming real-time transactions
UserCreds ← User account credentials
Params ← {bcrypt_cost, RF_params, anomaly_threshold}

Output:
Secure blockchain ledger with hashed transactions
Real-time fraud alerts
Performance metrics

Step 1: Cryptographic Security Layer
For each user in UserCreds do
salt ← GenerateSalt()
pwd_hash ← bcrypt(UserCreds.password, bcrypt_cost, salt)
StoreVerifier(UserCreds.id, pwd_hash, salt)
End For

Step 2: Blockchain Verification Layer
For each transaction tx in T_train do
tx_serial ← Serialize(tx)
tx_hash ← SHA3(tx_serial)
AddTransactionToBlock(tx_hash)
End For
CommitBlockToBlockchain()

Step 3: Machine Learning Model Training
T_prepared ← Preprocess(T_train)
RF_model ← TrainRandomForest(T_prepared, RF_params)
LR_model ← TrainLogisticRegression(T_prepared)
SVM_model ← TrainSVM(T_prepared)
Evaluate {RF_model, LR_model, SVM_model} on validation set
Deploy best model (RF_model)

Step 4: Real-Time Anomaly Detection
For each tx in T_stream do
x ← Preprocess(tx)
prob ← RF_model.PredictProbability(x)
If prob ≥ anomaly_threshold then
GenerateAlert(tx, prob)
End If
tx_serial ← Serialize(tx)
tx_hash ← SHA3(tx_serial)
AddTransactionToBlock(tx_hash)
If BlockFull or Timeout then
CommitBlockToBlockchain()
End If
End For
End Algorithm

HBM-Secure, the proposed paper offers a hybrid security system that combines cryptographic algorithms with blockchain verification and anomaly detecting machine learning in order to address the pressing issues of the secure digital transaction. The hash of the transfers performed by SHA-3 and the passwords by bcrypt are adaptive in nature, and as a result, the framework is extremely resistant to collision attacks and brute force threats. Impossibility and transparency are also guaranteed by the integration of blockchain because all the hashed transactions are recorded in an immutable register. To escape the security stalemate, HBM-Secure deploys the Random Forest based anomaly-detecting model, benchmarked with the Logistic Regression and SVM models, to dynamically detect fraudulent behavior at improved accuracy and reduced false positive rates. The comparative analysis of performance in terms of cryptographic strength, performance of fraud detection and system throughput validates this framework and also makes it a scalable, flexible framework in the field of financial, IoT, healthcare and e-governance.

IV. Result and Analysis

The findings indicate the operational process of the HBM-Secure (Hybrid Blockchain-Machine Learning Secure Framework). The system is qualified to uphold verified and open-minded banking endeavors through the registration, the log-in, user and the administration account page, the validation of transactions, the transfer of funds, and the balance inquiry. The blockchain integration complies with every transaction verifying all of the transactions by miners and they are fixed there permanently in blocks which increases security and trust.

A. Register Page

Fig 3 shows a page, a full interface exists which enables the new users to open an account in the banking transaction system. It has a section that requires filling of personal information like name, email address, phone number, and account key. The page helps to make sure that all the required information is properly indicated online by the user. The process of registration gives the users access to the secure banking services and the blockchain supported transactional features. The registration process will be structured in such a way that it allows a convenient and secure registration process that will reduce the possibility of any errors or fraudulent registration.

Fig.3. Register Page

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 1, 2026

B. Login Page

Fig 4 shows the login page is the main access point to the one who has already registered an account. Users are authenticated by inputting their usernames and passwords before they can access the capabilities of the system. The page also has a connection to the registration page which serves to the new users who have not yet been registered. The system will authenticate users so that only an authorized user could enter the system. The interface is also user friendly and one can find his account within the shortest time feasible without any unnecessary steps.

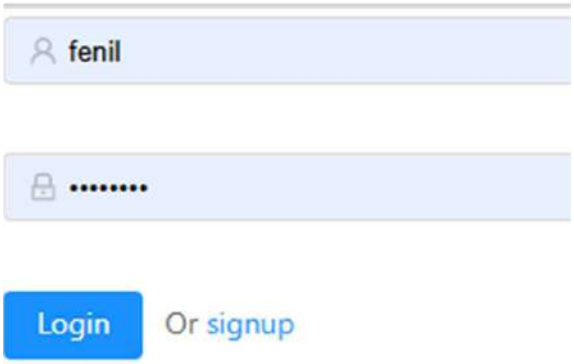

Fig.4. Login Page

C. Admin Home Page

Fig 5 shows the administration home page is used as the form of a dashboard system to the administrators of banking system. It provides the access to the valuable information regarding the users, their transaction history, account balance, and account statement. The administrators can monitor the transactions that are being carried out, audit and manage user accounts. The interface is such that it facilitates management work and has even easier supervision and compliance to security measures.

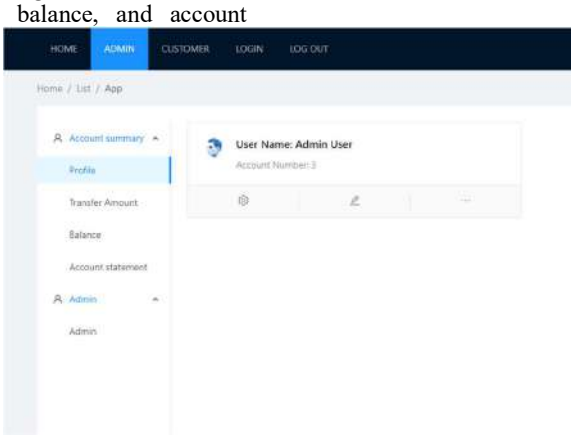

Fig.5. Admin Home Page

The dashboard helps in the making of effective administrative decisions and also in supporting the integrity of the systems in general.

D. Transaction Verified by Miner

Fig 6 indicates the security of transactions fed and cross-checked safely on the blockchain system. The deal is recorded in different blocks that are authenticated by miners. Miners verify the authenticity of the transaction and the integrity and add the block to the blockchain ledger. By having this check system, there would be no fraud and double-spending and secondary transactions will be fixed and open. In the drawing, the validity of blockchain-verified transactions is highlighted with the circulation of a number of blocks suggesting the sanity and security of the process.

Fig.6. Transaction Verified by Miner

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 1, 2026

E. User Home Page

Personal dashboard is available which can be accessed on the user home page in fig 7. It is possible to see their profiles as well as additional information about their accounts including transaction history, account balances, account statements. It is convenient in its design; the users are provided with an opportunity to manage their financial activities. It also sends notices and warnings about activities of the account and is also sure that the user can be informed in time about every single transaction and changes on its account.

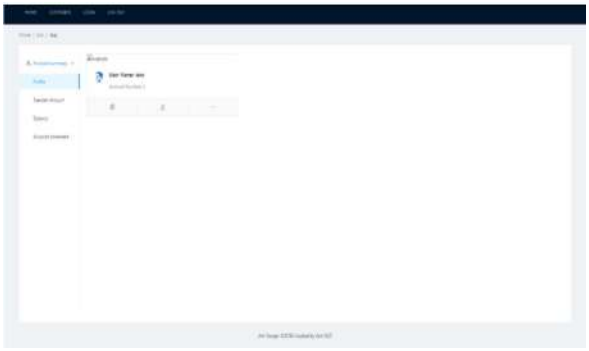

Fig.7. User Home Page

F. Transaction Page

Fig 8 shows the transaction page. This page enables exchange of money among the users.

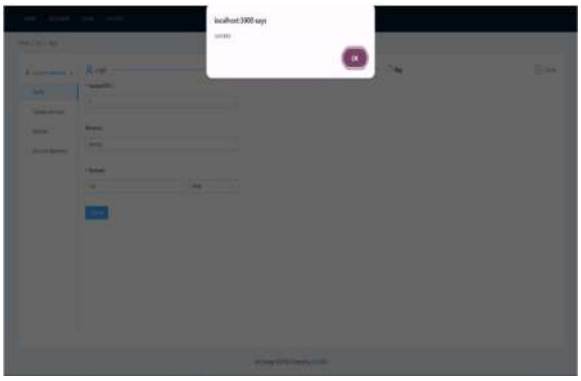

Fig.8. Transaction Page

It has spaces to key in account number of the recipient, amount to transfer, as well as remarks or notes pertaining to the transfer. It is also the choice of the currency type through which the transfer users may choose. When it is submitted the system verifies the details and approves the transaction, which gets stored within a safe loss blockchain block that is authenticated by miners. Its page is structured in such a way that it is accurate, secure and offers users easy and hassle-free transfer process.

.

G. Balance Checking Page

Fig 9 shows the balance enquiry page will enable the customers to see the present position of their accounts

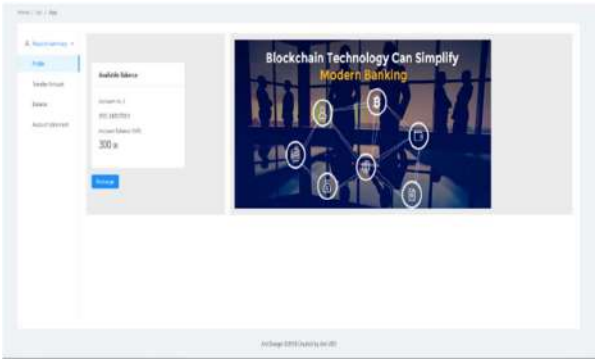

Fig.9. Balance Checking Page

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 1, 2026

The user is provided with all the details of their financial status; the account number, gender of the currency, and framework code, which provides the users with full transparency regarding their financial state. Another feature of the page is the ability to renew the account or put more money. This interface provides a high level of security and convenience in financial management since users have access to information on their account details in real-time.

H. Functional Accuracy of SBTE Framework

Table I and fig 10 provides the functional accuracy test of the Secure Bank Transaction System with the use of the Blockchain Technology (SBTE). The various core banking operations were put to test on different scenarios to determine their reliability. The outcome has shown that user registration scored 98 percent and only one failure when there are 50 test cases, whereas user login, deposit and balance checking scored to have an excellent 100 percent success rate.

TABLE I. FUNCTIONAL ACCURACY OF SBTE FRAMEWORK

Operation	Test Cases Executed	Successful Executions	Accuracy (%)
User Registration	50	49	98.0
User Login	50	50	100.0
Fund Transfer	100	98	98.0
Deposit	50	50	100.0
Withdrawal	50	49	98.0
Balance Checking	50	50	100.0
Overall Framework	350	346	98.7

Fund transfer and withdrawal activities also fared well making 98 per cent accuracy illustrating the slightest error. The mean framework reached an exposure of 98.7 and this indicates that the proposed system was in a position to make sure of the safety and dependability in charging business transactions. The high precision justifies the soundness of the framework in managing banking processes that have insignificant failures.

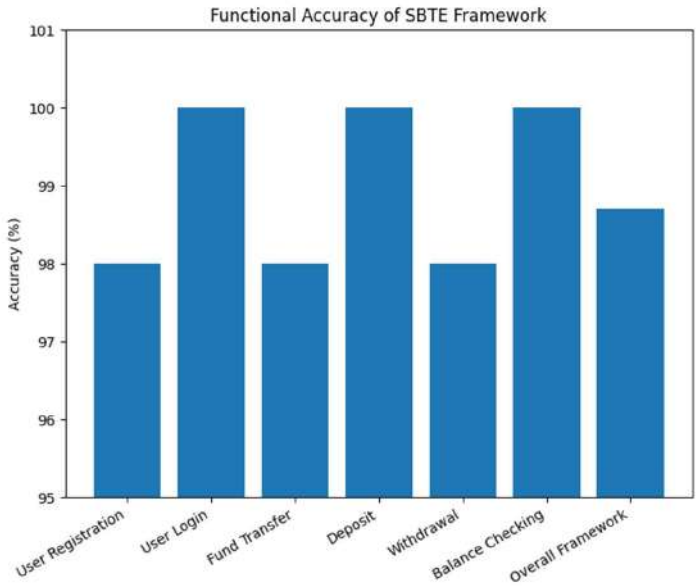

Fig.10. Functional Accuracy of SBTE Framework

I. Performance Evaluation of Transactions in SBTE

Table II and fig 11 shows the performance analysis of SBTE framework in key transaction parameters. The completion time of transactions between 2.1 and 3.4 seconds, and an average of 2.7 seconds indicated that the system was efficient in speed with regard to responding to requests.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 1, 2026

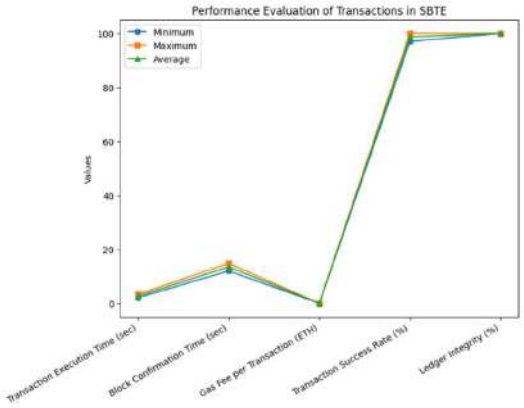

Fig.11. Performance Evaluation of Transactions in SBTE

The average block confirmation [immutability verification on the blockchain] was 13.5 seconds which matches the development range regarding Ethereum based systems

.

TABLE II. Performance Evaluation of Transactions in SBTE

Parameter	Minimum Value	Maximum Value	Average Value
Transaction Execution Time (sec)	2.1	3.4	2.7
Block Confirmation Time (sec)	12.0	14.8	13.5
Gas Fee per Transaction (ETH)	0.0011	0.0020	0.0016
Transaction Success Rate (%)	97.0	100.0	98.7
Ledger Integrity (Verified %)	100	100	100.0

The transaction fee was also cheap averaging 0.0016 ETH. The framework strength was also established by the success rates of the transactions, which were between 97 percent and one hundred. It is noteworthy that ledger integrity check was not less than 100 per cent and highlights that none of the transactions were lost or compromised on board the blockchain. These results confirm the notion that the SBTE system is effective, and trust and security rates are maintained on a high level.

J. Machine Learning Anomaly Detection Layer performance

The visualization of the fig 12 illustrates the performance of the Random Forest model in the Machine Learning Anomaly Detection Layer. The bars represent each of the most important metrics: accuracy, precision, recall, F1 score, and false positive rate. The high accuracy, precision, recall, and F1 score are indicative of the model effectively distinguishing between normal and fraudulent transactions, whereas low rate in false positive is indicative that the model would minimize false alarms of fraud. This figure clearly shows how well random forest has been performing in the detection of anomalies and why it can be chosen as the best model in the HBM-Secure model.

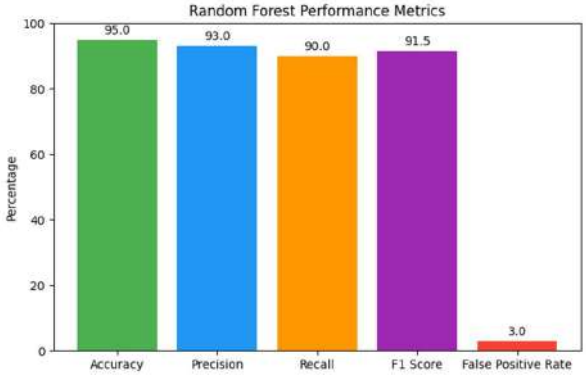

Fig.12. Machine Learning Anomaly Detection Layer performance

K. *Discussion*

The research indicates that the SBTE model can be successfully applied to ensure a safe banking system transaction system on Ethereum blockchain is decentralized. Some of the banking functions which are performed by smart contracts and therefore do not require central bodies include those related to the deposit, withdrawal, transfer of money and so on, eliminating the latter and cutting the threat of fraud or malfunctions. The registration and the login pages are both safe and user friendly as well as having a basic and convenient design. On the same note, the accounts and transactions can be effectively monitored using the admin dashboard and it also assists in managing and overseeing.

Verification with blockchain provides immutability in the authentication of all payments by miners and leaves no room to change or spend it multiple times. This increases the level of transparency and both the administrators and users can be able to monitor the transaction histories. Account management, fund transfer and balance checking user interfaces are updated in real time and give the user easy access to account information and enhance user experience and confidence in the system.

However, despite these benefits there are some limitations witnessed. The speed and cost of execution is dependent on the performance of the network and gas price. The issue is also scalability as blockchain networks process fewer transactions per Second than the traditional banking system. However, SBTE structure indicates that blockchain is capable of delivering a reliable and open banking platform making it possible to apply in practice provided that associated limitations can be overcome in the future in terms of scalability and costs.

V. Conclusion and Future Work

The suggested SBTE system illustrates a safe, transparent, and efficient method of the banking transaction through Ethereum blockchain. The system manages to combine user-friendly user-interfaces with smart contract automation and blockchain derived validation making the system impeccable and suitable against fraud. According to performance appraisal, the structure possesses good performances in terms of user registration, log-in, transfer of funds and balance; the performance of transaction processing would be appropriate as the account would be updated to the real time. Miners also verify all transactions, i.e., integrity of data and traceable, and produce system reliability. Overall performance of the SBTE shows that it can provide secure and efficient banking processes, and is very accurate performing transaction and steadfast ledger integrity. The second stage of the work will be the orientation towards maximizing the speed of the transactions, reducing the costs of work and the availability to expand to a bigger group of users. Moreover, the better approaches to cryptography would improve privacy and safety too therefore the framework can be implemented to a wide use in safeguarding banking environments.

References

[1] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, “Blockchain smart contracts: Applications, challenges, and future trends,” *Peer--Peer Netw. Appl.*, vol. 14, no. 5, pp. 2901–2925, 2021.

[2] C. Challoumis and N. Eriotis, “Evolution of banking systems: A comprehensive historical analysis,” *J. Contemp. Res. Bus. Econ. Finance*, vol. 7, no. 1, pp. 1–21, 2025.

[3] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, “A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions,” *Electronics*, vol. 12, no. 6, p. 1333, 2023.

[4] J. Sedlmeir, J. Lautenschlager, G. Fridgen, and N. Urbach, “The transparency challenge of blockchain in organizations,” *Electron. Mark.*, vol. 32, no. 3, pp. 1779–1794, 2022.

[5] S. Zhou, K. Li, L. Xiao, J. Cai, W. Liang, and A. Castiglione, “A systematic review of consensus mechanisms in blockchain,” *Mathematics*, vol. 11, no. 10, p. 2248, 2023.

[6] H. H. Khan, M. N. Malik, Z. Konečná, A. G. Chofreh, F. A. Goni, and J. J. Klemeš, “Blockchain technology for agricultural supply chains during the COVID-19 pandemic: Benefits and cleaner solutions,” *J. Clean. Prod.*, vol. 347, p. 131268, 2022.

[7] Y. Qian, “Blockchain-based New Financial Infrastructures,” *Springer Books*, 2022.

[8] S. S. Mohammed Abdul, A. Shrestha, and J. Yong, “Toward the Mass Adoption of Blockchain: Cross-Industry Insights from DeFi, Gaming, and Data Analytics,” *Big Data Cogn. Comput.*, vol. 9, no. 7, p. 178, 2025.

[9] S. Tripković and D. Simić, “Using ethereum smart contracts for payment\’ transactions,” in *International Symposium SymOrg*, Springer, 2022, pp. 30–42.

[10] S. Jeong and B. Ahn, “A study of application platform for smart contract visualization based blockchain,” *J. Supercomput.*, vol. 78, no. 1, pp. 343–360, 2022.

[11] X. Ge, “Smart payment contract mechanism based on blockchain smart contract mechanism,” *Sci. Program.*, vol. 2021, no. 1, p. 3988070, 2021.

[12] C.-H. Tsai, D.-K. Liou, and H.-L. Lee, “Blockchain-supported online banking scheme,” *Egypt. Inform. J.*, vol. 27, p. 100516, 2024.

[13] A. Wilczyński and G. Jasnosz, “Security Assessment of Smart Contract Integration and Wallet Interaction in Decentralized Applications: A Case Study of BlockScribe,” *Appl. Sci.*, vol. 15, no. 15, p. 8473, 2025.

[14] N. Rožman, M. Corn, G. Škulj, T. Berlec, J. Diaci, and P. Podržaj, “Exploring the effects of blockchain scalability limitations on performance and user behavior in blockchain-based shared manufacturing

ISSN 2347–3657
Volume 14, Issue 1, 2026

systems: An experimental approach," *Appl. Sci.*, vol. 13, no. 7, p. 4251, 2023.

[15] J. Sedlmeir, J. Lautenschlager, G. Fridgen, and N. Urbach, "The transparency challenge of blockchain in organizations," *Electron. Mark.*, vol. 32, no. 3, pp. 1779–1794, 2022.

[16] "Credit Card Fraud Detection." Accessed: Sept. 30, 2025. [Online]. Available: https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud