

Enhanced IoT Supported Blockchain Information Sharing Framework for Banking Transaction Fraud Detection and Workload Design

Narasimha Rao Thota^{1,*}

¹Vice President, BNY, Jersey City, NJ

Corresponding Author: Narasimha Rao Thota. Email: thotanrao@gmail.com

Received: 15/07/2026; Revised: 30/07/2026; Accepted: 28/08/2026; Published: 30/09/2026

<https://doi.org/10.69996/jsihs.2026012>

Abstract: Power BI is essential for detecting money laundering in Kaggle banking fraud datasets. Securing smart contracts against quantum threats is vital. Regular retraining of machine learning models and AI-blockchain integration enhance secure data sharing and confidentiality in banking. To overcome this issue a new model Enhanced IoT Supported Blockchain Information Sharing and Workload Design (EIBIWD). To ensure consistent data presentation and restrict access, the information sharing process utilizes the User Data Requirement (UDR) procedure and the Universal Access Controller (UAC) methodology. The PaySim models real-life financial scenarios, including interbank transactions, micropayments, batch settlements, and fraud. Workload patterns encompass arrival rate, execution time, transaction amount, account details, balance, fraud indicators, micropayment limits, transactions per second, endorsing peers, and batch parameters. IoT lattice-based blockchain provides quantum-resistant security for IoT devices, enhancing financial applications through cryptography, smart contracts, and secure key exchanges. The HyperNet model facilitates secure data control in the Private Data Center (PDC), with UDR and UAC ensuring data consistency. The PaySim model addresses financial activities, focusing on metrics like fraud indicators and transaction rates. The IoTBlockchain System employs this technology for secure financial operations. The performance analysis is transaction, latency, throughput, validation of digital signature calculations.

Keywords: Banking Transaction Fraud Detection, Universal Access Controller (UAC), User Data Requirement (UDR), Private Data Center (PDC), and IoT-Blockchain

1. Introduction

Conventional fraud detection methods often generate excessive false positives, increasing investigation costs and undermining financial monitoring. Globalization has led to a surge in cross-border transactions involving banks, insurance companies, and customs officers. Factors like transaction rates, execution times, values, account details, and fraud indicators affect transaction workloads [1]. The information sharing process includes UDR and UAC to ensure consistent data representation and authorized access across platforms. The PaySim model effectively represents real-life financial scenarios, including batch settlements, interbank transfers, micropayments, and fraud control [2]. This proposed IoT-Blockchain system outlines operational dynamics and the transaction process using mathematical workload formulation. Additionally, machine learning and deep learning are increasingly employed for financial data analysis, fraud detection, and identifying questionable transactions. Implementing complex models poses challenges in computing, scalability, maintenance, and integration [3]. Model deployment complicates workflows due to the need for ongoing management of databases, protocols, upgrades, and outputs. Centralized processing raises data ownership, privacy, and trust



issues, though cloud solutions can aid deployment. Additionally, private data from cyber-physical-social environments must be protected by secure access control systems and tamper-proof records [4]. Blockchain provides a decentralized, tamper-proof transaction record that ensures financial traceability and auditability through an immutable peer-to-peer ledger. Smart contracts streamline workflows by minimizing human oversight. However, challenges in cryptographic security, interoperability, smart contract management, and regulatory compliance limit financial blockchain applications. Quantum computers will also compromise traditional cryptographic systems. Cross-border smart contracts require added transaction protection due to differing regulations [5]. Code vulnerabilities can lead to unauthorized term changes, data leaks, double-spending, and loss of user confidence. Existing approaches must adopt enhanced security mechanisms to safeguard against these threats. Terrorist funding and money laundering undermine financial system secrecy. Criminals, including drug dealers and extortionists, generate illegal funds, and the allure of cryptocurrencies—swift transactions—attracts public interest, as KYC and AML measures fail to deter these crimes [6].

The research introduces EIBIWD, a model enhancing financial transaction management by integrating blockchain, IoT, and lattice-based post-quantum cryptography for improved security, featuring quantum-resistant key exchange and authentication via Dilithium signatures and Kyber key encapsulation. The major contribution of the paper is below. The integration of blockchain and IoT enhances financial services by improving workload distribution, ensuring transaction trust, fostering accountability, and facilitating efficient information exchange. A proposed security approach utilizes lattice-based blockchain to protect confidential transactions against quantum attacks, featuring secure key exchange, authentication, and transaction verification with Dilithium signatures and Kyber encapsulation. To ensure comprehensive security, the design incorporates multiple encryption layers, smart contracts, adherence to standards, post-quantum cost estimation, and quantum-resistant address derivation. They created a HyperNet-powered PDC for secure data sharing among authorized financial institutions, implementing access control and data normalization. Microsoft Power BI is utilized for visualization, query processing, and real-time transaction tracking. This framework manages micro-payments, cross-bank operations, batch settlements, and fraud-related tasks, influenced by transaction rate, execution time, value, account holder details, and processing parameters.

2. Related Works

In [7], the author suggested a Zero Trust Federated Learning framework with GAN-based anomaly detection for financial fraud. The method improves privacy and fraud detection using synthetic data augmentation. However, GAN training and federated learning increase computational and communication costs. In [8], the author offered a face recognition-based protocol for secure online transactions. The method improves transaction security through biometric authentication. However, recognition accuracy may be affected by poor image quality and varying facial conditions. In [9], the author reviewed machine learning methods for fraud detection in Ethereum blockchain transactions. The study highlights the effectiveness of ML techniques in identifying suspicious blockchain activities. However, the review indicates challenges related to evolving fraud patterns and limited labelled data. In [10], the author recommended a blockchain anomaly detection model using GAN and autoencoder techniques. The method improves abnormal transaction detection through feature learning and synthetic data generation. However, the combined architecture increases computational complexity and training requirements. In [11], the author developed an ensemble tree-based model for digital financial fraud detection. The approach improves fraud classification by combining multiple decision-tree

models. However, ensemble models can require higher computational resources and may have reduced interpretability.

In [12], the author anticipated federated micro-expression mining with multimodal metadata fusion for Deepfake fraud detection in video-KYC systems. The method enhances privacy and improves Deepfake detection by combining visual and metadata features. However, multimodal processing and federated training increase computational and communication overhead. In [13], the author developed an AI-driven FinTech framework for risk assessment and fraud detection. The approach enables intelligent analysis of financial data for improved fraud identification and risk management. However, its performance depends on data quality, model complexity, and reliable financial datasets. In [14], the author applied machine learning techniques to detect fraud in IoT-based credit card transaction data. The method supports automated fraud identification using transaction-related features. However, IoT-generated data can introduce noise, security concerns, and scalability challenges. In [15], the author recommended TabNet, an adaptive deep learning architecture, for bank transaction fraud prediction. The model improves fraud prediction through attention-based feature selection and interpretable learning. However, TabNet may require substantial training data and computational resources for effective performance.

3. Proposed EIBIWD Model

This proposed model is developed to enhance the information sharing and workload design performance of the banking system with the presence of the enhanced IoT supported Blockchain technology where its workflow is illustrated in the figure 1. The core modules of this process are dataset details, IoT lattice-based blockchain technology, IoT-Blockchain based information sharing process, IoT-Blockchain transaction workload details and performance analysis.

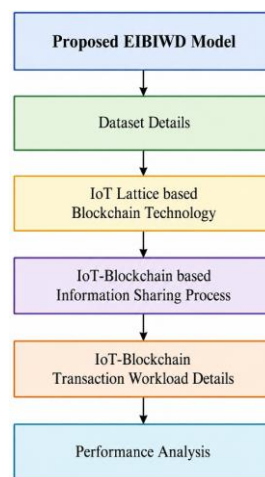


Figure 1: EIBIWD Model Architecture

3.1 Dataset Details

The considered dataset for this analysis is the financial services datasets which includes the presence of monetary transaction data of the nascent domain. This dataset mainly concentrates on the money laundering activities and its fraud and the detection process including the PaySim simulator. This dataset consists of the details about the systematic procedure, type, amount, organization name, old balance, current balance and fraud flagged details. For the details analysis of the process the concept of Microsoft Power BI integration is performed where

its details are explained in the table 1.

Table 1: Microsoft Power BI Integration

Component	Description
Power BI Reports	Interactive monitoring, visualization, Q&A, and model tracking
Query Processing	Power BI → Connector → Azure AD → Authorized User
SSAS Security	Role-based permissions applied through SSAS
Data Retrieval	Local SSAS cube queried with cached connections
Data Sources	Local sources via Power BI Desktop / Excel
Personal Gateway	Enables data synchronization and report refresh
Azure Integration	Connects Azure SQL Database, Auditing, and Stream Analytics
Stream Analytics	Processes streaming data and updates Power BI dashboards in real time
Overall Function	Integrated, secure, and real-time business intelligence

3.2 IoT Lattice based Blockchain Technology

Lattice technology is an advanced model which is developed from the quantum computing process and it mainly concentrates on the functionality of cryptographic primitives which is present in the quantum computing. It consists of various features such as identity, digital signatures, consensus and as well an intelligent contract execution. This model plays under three main levels such as cryptography layer, smart contract layer and compliance layer where its process is illustrated in the figure 2.

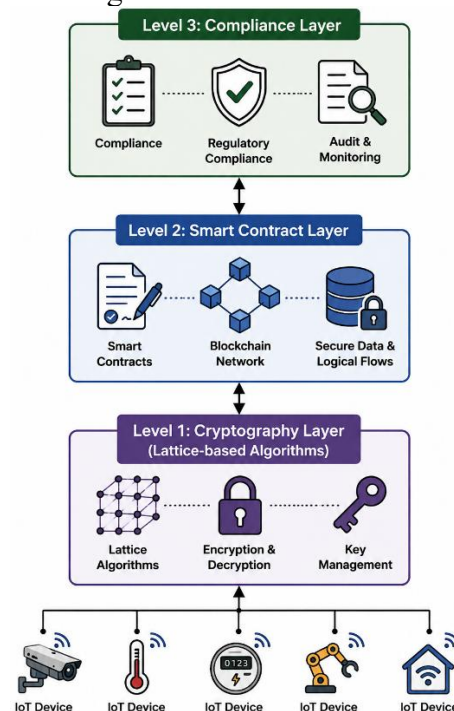


Figure 2: IoT Lattice BT Levels

This model is effective for the straight forward financial applications and it consists of quantum-resistant regular security. This method helps to maintain the integrity of the smart contracts based in the blockchain safety. At the initial condition, data encryption is performed in

an effective way, followed by that the process of Kyber and Dilithium algorithms are utilized to performed a key exchange operation based in quantum-safer model and as well as the digital signature process. Then the running of smart contracts is performed in the second layer. In the final stage, compliance is considered which includes the major processes such as anti-money laundering and data localization and as well as an effective analysis about the customer. This process results in the enhancement of the security, scalability and decentralization of the financial applications.

At this condition, the process of Kyber and Dilithium algorithms are elaborated where the Kyber model performs key encapsulation process and the Dilithium model performs digital signatures which is developed with the presence of the post-quantum cryptography. The intelligent contacts and the transaction information are secured using the quantum-resistant authentication process which integrates the IoT supported blockchain technology through the libraries and APIs. The key operations of these modules are quantum adversary analysis, intelligent contacts analysis through cross-border financial details and so on. The mathematical expression for the calculation of making mistakes are given in the equation (1), which is based on the public component (ql) and it gets sampled from the infinite field ($B.t$) where its limitations are analysed through ($f \bmod r$) (prime integer). In the equation (1), the generation of lattice key is given followed by that in the equation (2), the Kyber key related encapsulation is given.

$$ql = B.t + f \bmod r \quad (1)$$

$$du = ql.s + f' \bmod r \quad (2)$$

The equation (2) is measured using the principle of Key Encapsulation Mechanism (KEM), where the term, du implies the transient random vector, $ql.s$ implies the secret/public key and the term $f' \bmod r$ implies the possible lattice assaults. In the equation (3) and (4), the calculation of Dilithium signature generation and verification is performed.

$$a = z + t.d \quad (3)$$

$$x' = B.a - u.d \bmod p \quad (4)$$

The equation (3), mainly explains about the signature response creation process and here the term a implies the nonce vector, t implies the signature of the random samples, z implies the secret key and the term d implies the z based hash value which are all present in the cryptographic commitment. In the (4), the proper explanation about the received signature is present and it is employed in the recreation process of the term x' . Here the term $\bmod p$ implies the verification procedure and as well it gets multiplied by the public matrix $B.a$ which is the primary factor used in the process of key generation of the signature responses denoted as $u.d$. In the equation (5), the mathematical expression for the calculation of quantum resistant based address derivations is explained.

$$addr = I(ql||ma) \quad (5)$$

This equation (5), mainly concentrates in the process of quantum computing supported address derivation process in the BT systems. In order to construct the BC, address it gets combined with the secured hash algorithm ql . In the equation (6), the overhead calculation of the PQ estimation cost with the presence of the gas cost intelligent contract.

$$H_{qr} = H_{base} + b.|a| + \epsilon.|qp| \quad (6)$$

In the equation (6), the term H_{qr} implies the gas expenses which is related to the H_{base} (base cost) and the $b.|a|$ (extra cost) and it gets linked with the post-quantum cryptography. With the presence of the term $\epsilon.|qp|$, the calculation of on-chain processing and computational

costs gets reduced and it is then scaled through the coefficient. In the equation (7), the calculation of the latency is given in terms of the transaction process.

$$U_{total} = U_{disg} + U_{enco} + U_{veri} + U_{upd} \quad (7)$$

In the equation (7), the term U_{total} implies the total latency analysis according to the transaction. The other components such as U_{disg} , U_{enco} , U_{veri} and U_{upd} implies the factors such as Kyber key encapsulation, verification and network propagation. Through this analysis the security and integrity of the financial system is enhanced. Followed by that the concept of layer adaption and security enhancement is elaborated in the table 2.

Table 2: Layer Adaption and Security Enhancement

Layer / Component	Function / Description
Consensus Engine	PQ signature verification for quantum-safe block validation
Identity Layer	Hash addresses → Dilithium-based PQ public keys
Transaction Validation	Quantum-safe authentication and validation
Intelligent Contracts	PQ-compatible compilers, runtimes, larger keys/signatures
Block Processing	Secure transaction authentication, proposing & finalization
Ledger Security	Quantum-safe finalization without throughput loss
Compatibility Wrapper	Supports legacy transactions during PQ migration
Endpoints	Classical endpoints → post-Quantum endpoints
Identity Verification	Dilithium signatures authenticate participants
Key Management	Lattice-based secure key protection
Contract Protection	Encryption secures contract code and state
Execution Logs	Tamper-proof smart-contract activity records
Randomization	Entropy-based secure randomness prevents predictable logic
Overall Security	Reduce impersonation, replay and contract-switching attacks

3.3 IoT-Blockchain based Information Sharing Process

HyperNet supported Private Data Center (PDC) model is utilized for this integrated blockchain process and it mainly concentrates on the security mechanisms of the sharing information. The proper protection for the physical information is provided by the data center (DC) which is developed with the presence of the open source (AI) technology. Through the process of PDC, the secured data control is provided in an effective way and as well it consists of two main elements which concentrates on uniform access control such as User Data Requirement (UDR) and Universal Access (UAC) where it details are given in the table 3. The network model of the information sharing process of the IoT-Blockchain network is illustrated in the figure 3.

Table 3: Details about UDR and UAC

User Data Requirement (UDR)	Universal Access (UAC)
Standardizes data representation	Standardizes access control
Describes and processes data uniformly	Controls data accessibility
Supports different data formats/platforms	Supports multiple platforms
Enables data confirmation/processing	Manages read, write, attach,

programs	etc
Resolves data-style inconsistencies	Controls users, groups, and programs
Provides consistent data requirements	Determines permitted data requests
Supports data identification through PDC	Provides authorization through PDC

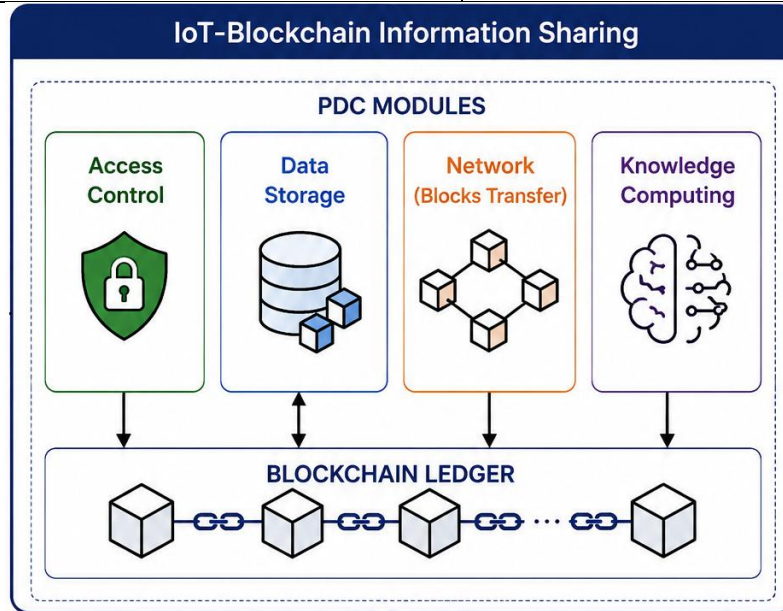


Figure 3: IoT-Blockchain Information Sharing

3.4 IoT-Blockchain Transaction Workload Details

To attain high accuracy in the realistic financial transaction is the primary concentration of this transaction workload analysis process which includes the PaySim simulator and it mainly concentrates on the high-frequency micro-payments, cross-bank transactions, batch settlements and fraud related analysis. The symbols and its description which are used in this section is explained in the table 4.

Table 4: Symbols and Description

Symbols	Description
W_k	Workload entry
T_i	Individual transaction
C_k	Workload category
δ_k	Transaction arrival rate
t_k	Workload execution time
A_i	Transaction amount
O_i and R_j	Origin and destination account
$B_{orig,i}$ and $B_{dest,i}$	Account balances,
F_j	Fraud flag.
α	Micro- payment threshold
W_{micro}	Micro-payment transactions collection
t_{micro}	Workload execution time

δ_{micro}	Transactions per second
$B_{orig}(i)$	Sending bank transaction-based account identification
$B_{dest}(i)$	Receiver bank transaction-based account identification
E_{cross}	Endorsing peers set (Validation purpose)
P_a	Home bankpeer nodes
P_b	Target bankpeer nodes
$Batch_j$	Batch j based total transaction value
S_j	Batch j based transaction set
$isFraud_i$	Fraud related binary marker
W_{fraud}	Fraud workloads

Using the above symbols and description the expressions for the calculation of the transaction workload process is given in the equations (8) to (14).

$$W_k = \{T_i | T_i \in C_k, \delta_k = \frac{|W_k|}{t_k}, t_k, A_i, O_i, R_i, B_{orig,i}, B_{dest,i}, F_i\} \quad (8)$$

$$A_i \leq \alpha \quad (9)$$

$$\delta_{micro} = \frac{|W_{micro}|}{t_{micro}} \quad (10)$$

$$B_{orig}(i) \neq B_{dest}(i) \quad (11)$$

$$E_{cross} = P_a \cap P_b \quad (12)$$

$$Batch_j = \sum_{i \in S_j} A_i \quad (13)$$

$$W_{fraud} = \{T_i | isFraud_i = 1\} \quad (14)$$

This workload analysis improves the system capability which leads to the enhancement of the security and transparency in the financial transactions with the IoT-blockchain technology.

4. Simulation Environment

This proposed model is mainly developed to identify and neglect the banking transaction fraud and it is performed in the python tools. The measured results of the proposed EIBIWD are compared with the existing models such as IRAFD [13], DFICM [14] and PBTFT [15-16].

4.1 Validation of Digital Signature

At 20 samples, EIBIWD achieves 45.21%, outperforming IRAFD by 39% (15.36%), DFICM by 23% (21.49%), and PBTFT by 6.4% (33.12%). At 80 samples, EIBIWD surpasses IRAFD by 59.46%, DFICM by 66.72%, and PBTFT by 83.46%. The hybrid security model combines quantum-resistant signatures and lattice-based blockchain security, reaching a 96.77% validation rate at 100 samples, as represented in figure 4 and table 5. The layered security framework integrates signature validation with identity and transaction verification, consensus methods, and secure processing, enabling increased transaction volume and validation. This approach enhances security through blockchain, IoT, and post-quantum cryptography.

Table 5: Validation of Digital Signature Measure

Number of Samples	IRAFD	DFICM	PBTFT	EIBIWD
20	15.36	21.49	33.12	45.21
40	31.49	45.47	56.72	65.89
60	46.28	59.46	76.44	84.23
80	59.46	66.72	83.46	89.64
100	68.22	81.49	86.99	96.77

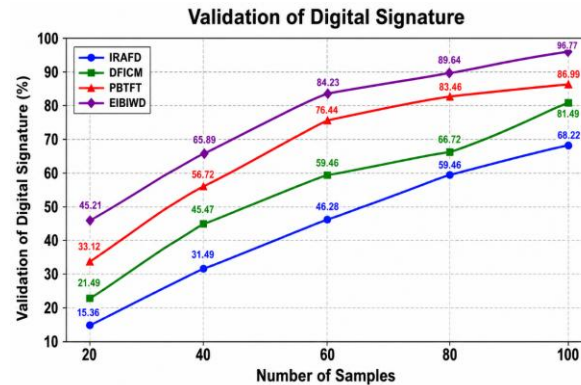


Figure 4: Validation of Digital Signature Calculation

4.2 Throughput Calculation

The Y-axis shows throughput in seconds and the X-axis displays various methods. The EIBIWD model outperforms with an average of 96.28 seconds, higher than IRAFD's 61.84 seconds. It supports real-time monitoring of financial operations like batch settlements and fraud detection to prevent business interruption. Blockchain validation ensures accurate data handling among network participants, while lattice-based security enables authentic transaction checks without impacting processing workload, as shown in figure 5 and table 6. Smart contracts enhance consistency by reducing manual transactions, facilitating secure data transfer in the IoT-Blockchain environment for better transaction coordination.

Table 6: Throughput Measure

Methods	IRAFD	DFICM	PBTFT	EIBIWD
Throughput (sec)	61.84	78.46	84.66	96.28

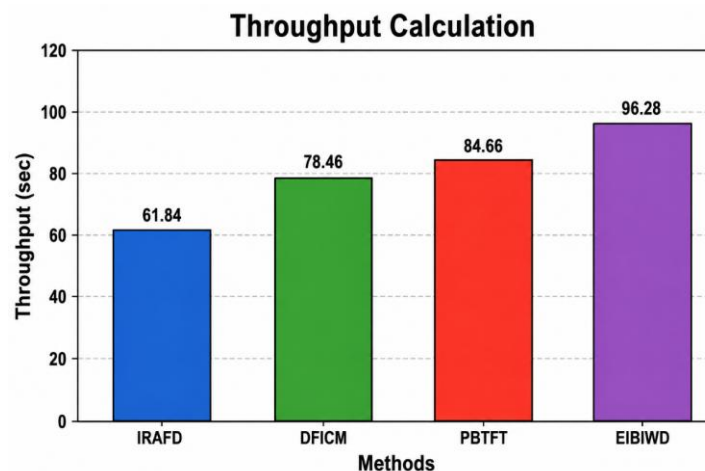


Figure 5: Throughput Calculation

4.3 Transaction Processing Latency Calculation

The Y-axis represents transaction time in seconds, while the X-axis shows different techniques. The EIBIWD model achieves the best result at 0.012 seconds, compared to IRAFD's 0.035 seconds. This solution leverages blockchain and IoT for secure data sharing and efficient processing, considering transaction arrivals, execution time, amounts, account data, and fraud workloads. The financial data remains unchanged due to verified blockchain transactions. Smart contracts reduce delays through automation, as represented in figure 6 and table 7. Quantum-

resistant authentication protects transactions from hackers until at least the end of the century. The system uses Dilithium digital signatures and Kyber key encapsulation for secure communication, enabling EIBIWD to process transactions in just 0.012 seconds.

Table 7: Latency Measure

Methods	IRAFD	DFICM	PBTFT	EIBIWD
Latency (sec)	0.035	0.027	0.021	0.012

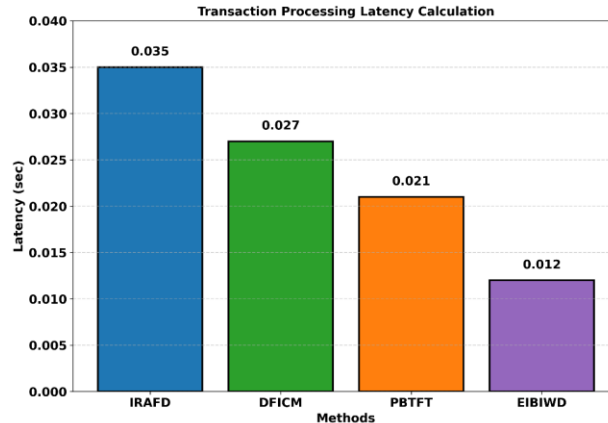


Figure 6: Latency Calculation

4.4 Transaction Calculation

The Y-axis shows transaction duration in seconds, while the X-axis presents various approaches. Using blockchain and IoT in EIBIWD architecture records a maximum duration of 435.69 seconds, compared to 325.54 seconds for IRAFD. Blockchain enables decentralized record-keeping and transaction validation, while smart contracts ensure reliable, automated execution. This architecture utilizes a quantum-resistant lattice-based blockchain for enhanced transaction security, supported by Dilithium digital signatures and Kyber key encapsulation for improved key management and validation, as shown in figure 7 and table 8.

Table 8: Transaction Measure

Methods	IRAFD	DFICM	PBTFT	EIBIWD
Transaction (sec)	325.54	389.54	402.89	435.69

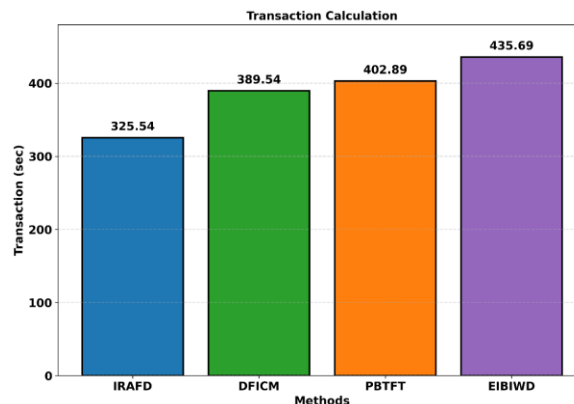


Figure 7: Transaction Calculation

5. Conclusion

The integration of blockchain with IoT aims to establish a secure and transparent

framework for managing financial transactions. This system enables safe data processing, including transaction details and fraud detection, while incorporating Microsoft Power BI for interactive visualization and live tracking. Quantum-resistant cryptographic methods like Dilithium and Kyber, along with IoT-based blockchain, safeguard key exchange, authentication, and transaction verification against powerful adversaries. This multi-tier structure ensures secure financial transactions through cryptography, smart contracts, and regulatory compliance, enabling tamper-proof execution records, consensus security, identity verification, contract protection, and quantum-safe address keys. UDR and UAC enable regulated data sharing via a HyperNet-supported PDC, promoting financial platform interoperability and a common data format. Transaction workloads reflect typical banking scenarios, including micro-payments, inter-bank transactions, batch settlements, and fraud detection, analyzed by transaction rate, execution time, and fraud indicators. EIBIWD achieves 45.21% accuracy at 20 samples, surpassing IRAFD by 39%, DFICM by 23%, and PBTFT by 6.4%. At 80 samples, it exceeds IRAFD by 59.46%, DFICM by 66.72%, and PBTFT by 83.46%. The hybrid model, combining quantum-resistant signatures with lattice-based blockchain security, reaches a 96.77% validation rate at 100 samples and processes faster than IRAFD, taking 96.28 seconds. It allows real-time financial monitoring, achieving 0.012 seconds versus IRAFD's 0.035 seconds. EIBIWD uses blockchain and IoT for secure data sharing, preserving financial data integrity, with a maximum duration of 435.69 seconds compared to IRAFD's 325.54 seconds. Future research should leverage banking datasets, consensus dynamics, adjustable workload distribution, and AI for anomaly detection, while evaluating frameworks for banking, regulations, and scaling IoT post-quantum cryptography to enhance reliability.

Acknowledgment: 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] Neelam Navya Sri and N. Ramana Reddy, "Real-Time Credit Card Fraud Detection Using AdaBoost," *FMEP*, vol. 1, no. 3, pp. 66–77, 2025.
- [2] D. I. Hasan, M. H. Abd Alsadh, H. M. Shakir, H. E. Mahmood, A. A. Ahmed, M. Abdeldayem and N. J. Ibrahim, "Quantum-resistant blockchain protocol for secure smart contracts in cross-border finance," *Procedia Computer Science*, vol. 275, pp. 855–866, 2026.
- [3] E. Oztemel and M. Isik, "The deployment processes of credit card fraud decision models developed with artificial intelligence techniques," *Procedia Computer Science*, vol. 265, pp. 566–571, 2025.
- [4] Erugu Saidulu and S. Rajender, "Securing Banking Transactions with Blockchain: A Tokenless Approach," *FMEP*, vol. 1, no. 3, pp. 78–92, 2025.
- [5] T. Felipe, M. Kaya, S. Mathews, and R. T. de Oliveira, "Rethinking digital transformation in commercial banking: A longitudinal analysis of business model innovation," *Digital Business*, vol. 6, no. 2, 2026.
- [6] B. Zheng, "Integrating blockchain technology with financial systems to enhance transparency and efficiency," *Kuwait Journal of Science*, vol. 53, no. 3, 2026.
- [7] A. Alenizi, S. Mishra and A. Baihan, "Enhancing secure financial transactions through the synergy of blockchain and artificial intelligence," *Ain Shams Engineering Journal*, vol. 15, no. 6, 2024.

-
- [8] A. Shees and S. Zubair, “Zero trust federated learning with GAN-augmented anomaly detection for financial fraud,” *Procedia Computer Science*, vol. 283, pp. 1472–1482, 2026.
 - [9] Rudra Bhanusri and N. Ramana Reddy, “Fraud Detection in Banking Transactions Using Machine Learning,” *IJARI*, vol. 13, no. 3, pp. 27–36, 2025.
 - [10] J. Crisóstomo, F. Bação, and V. Lobo, “Machine learning methods for fraud detection within Ethereum blockchain—A review,” *Blockchain: Research and Applications*, 2026.
 - [11] A. Xiong, C. Qiao, W. Li, D. Wang, D. Li, B. Gao, and W. Wang, “Block-chain abnormal transaction detection method based on generative adversarial network and autoencoder,” *High-Confidence Computing*, vol. 5, no. 4, 2025.
 - [12] T. Cai and X. Yang, “Digital financial fraud detection using ensemble tree model,” *Procedia Computer Science*, vol. 281, pp. 1449–1455, 2026.
 - [13] R. Rawat, A. Rawat, S. Gupta, S. A. R. Albert, T. M. Thiyaagu, H. Rawat, and A. Rajavat, “Federated micro-expression mining and multi-modal metadata fusion for Deepfake fraud detection in ubiquitous financial video-KYC systems at IoT network,” *Franklin Open*, vol. 14, 2026.
 - [14] G. G. Battu, M. Garg, S. Dey, K. Kaushik, R. Kumawat, and M. Soni, “AI-driven FinTech: Intelligent risk assessment and fraud detection in digital financial ecosystems,” *Procedia Computer Science*, vol. 282, pp. 2667–2677, 2026.
 - [15] M. N. Alatawi, “Detection of fraud in IoT based credit card collected dataset using machine learning,” *Machine Learning with Applications*, vol. 19, 2025.
 - [16] B. S. Prashanth, M. Kumar, A. Hoque, N. Al Muraqab, I. A. Moonesar, U. C. Braendle, and A. Rao, “Prediction of bank transaction fraud using TabNet—an adaptive deep learning architecture,” *International Review of Economics & Finance*, vol. 106, 2026