Journal of Theoretical and Applied Information Technology
15th September 2026. Vol.104. No.17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AI-ADAPTIVE FEDERATED BLOCKCHAIN (AFBCHAIN): DYNAMIC RL-OPTIMIZED CONSENSUS AND XAI-ENHANCED FRAUD DETECTION FOR ULTRA-SECURE, SCALABLE DIGITAL PAYMENTS

VOREM KISHORE[1], SRIKANTH BHYRAPUNENI[2], DR. NARESH KUMAR BHAGAVATHAM[3], VENKATA BALA ANNAPURNA P[4], DR K LAKSHMAIAH[5], MOHANA PRASAD M[6], DR. N. SATHEESH[7*]

[1]CSE - (AIML & IOT), R & AI, VNR Vignana Jyothi Institute of Engineering and Technology, Medchal - Malkajgiri, Hyderabad - 500118, Telangana, India.
[2]Associate professor, Department of CSE (IoT & CSBT), PACE Institute of Technology and Sciences, Ongole - 523272, AP, Inida.
[3]Associate professor, Department of CSE, Vignana Bharathi Institute of Technology, Avushapur, Hyderabad -501301, Inida.
[4]Venkata Bala Annapurna P, Assistant professor, Department of AI&ML, Aditya University, Surrampalem - 533437, AP, India.
[5]Professor and HOD, Department of CSE, Ashoka Women's Engineering College, Kurnool - 518001, AP, Inida.
[6]Assistant Professor, Department of AIML, QIS College of Engineering and Technology, Ongole - 523001, AP, Inida.
[7*]Professor, Department of Computer Science and Engineering, SCSE, FET, Jain Global Campus, Jain (Deemed-to-be University), Bangalore, Karnataka, India.
Email: [1]kishore_v@vnrvjiet.in, [2]srikanthbt3010@gmail.com, [3]bhagavatham.nareshkumar@vbithyd.ac.in, [4]annapurnap@adityauniversity.in, [5]klakshmaiah78@gmail.com, [6]mohanaprasad.m@qiscet.edu.in, [7*]nsatheesh1983@gmail.com

ABSTRACT

Undoubtedly, there is a pressing need to create secure, scalable and decision-making payment systems in the age of rising cyber threats and boundless digital financial innovation. Given this fact, this paper introduces AFBChain, a state-of-the-art federated blockchain platform aimed at enhancing the efficiency and security of transactions and fraud detection powered by Hyperledger Fabric, reinforcement learning (RL), federated learning (FL), and explainable AI (XAI). AFBChain essentially operates a Proof-of-Intelligence (PoI) consensus mechanism and has opted to make the switch between PBFT and PoS and DPoS protocols into a Markov Decision Process (MDP), which is adept at adaptively switching choice according to the current network conditions to improve the through-put around 25 percent and decrease latency by 20 percent compared to Ethereum baselines. To ease fraud-detection and privacy-preserving results of above 95% accuracy, FL is inspired by deep-learning models, Gaussian Mixture Models, can be used to provide fraud-detection results, and SHAP and LIME models can be used to explain the constructed anomaly-detection knowledge. Also included in the framework will be dynamic sharding with the help of an artificial intelligence-based system, extreme audits of smart contracts to vulnerabilities of reentrancy, as well as decentralized automated market-making mechanisms in DeFi using RL by reducing slippage by 17.5%. The throughputs, scalability and security improvements are measured using the PAI-BC index. Overall, AFBChain has proven to be better than traditional blockchains, providing a stable and transparent system for the DeFi-based ecosystems, cross-chain payment and central bank digital currency.

Keywords: *AI-Blockchain Symbiosis; RL-Adaptive Consensus; Federated XAI Fraud; Dynamic Sharding Payments; DeFi Liquidity Optimization*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1. INTRODUCTION

As the financial world has become a global entity in which trillions of dollars are transacted annually by digital means, the convergence has also made the system more susceptible to the risks of cyber security threats and laid bare the limitations of using legacy infrastructures and systems to enable financial transactions. The rapidly growing volume of transactions and payments, along with complicate, high-tech fraud schemes, make it difficult for traditional centralized financial markets to efficiently handle this influx of transactions and payments across borders, with greater transparency. Blockchain technology with its decentralized ledger, cryptographical protection, and even impossibility of tamper could be a solution that suited well to ensure tamper-proof transactions ledger without reliance of trusted parties [1]. Despite this, the greatest advantages of blockchain systems, however, these solutions are also subject to some significant challenges in terms of performance and security. As an example, Bitcoin is known to have an approximate transaction per second rate of around 7 transactions per second (TPS) whereas Ethereum has around fifteen to thirty transaction per second (TPS) before the implementation of the Layer-2 scaling solutions which makes them insufficient to support large-scale international payment applications [2]. In addition to the scaling man limits, classical consensus algorithms such as Proof of Work (PoW), are associated with considerable energy consumption, latency and susceptibility to attacks and 51% consensus attack as it could compromise the trust of the network users [3]. With the current transformations of digital finance, which include decentralized finance (DeFi), tokenized assets and central bank digital currencies (CBDCs), there is a growing need of intelligent blockchain infrastructures which can dynamically optimize their performance whilst maintaining strong security assurance [4].

Recent developments in artificial intelligence (AI) and particularly deep learning (DL) and reinforcement learning (RL) might be an attractive addition to the communication technology of blockchain. The AI systems can also process vast quantities of transaction data, detect unusual patterns of activity and real-time network management [5]. A case in point is machine-learning behaviours to detect suspicious financial operations, e.g., phishing, money laundering or double-spending attacks, through the learning of behavioral trends in transactions [6]. More specifically, reinforcement learning offers an adaptive decision-making mechanism that enables blockchain networks to adaptively vary the approach adopted for consensus as a function of the network conditions such as transaction load, node reliability, latency constraints [7]. However, even with these advancements, many of these AI-blockchain solutions already exist today and focus on specific uses of a chain, for instance, centralized fraud detection or fixed hybrid consensus algorithms, but not on using AI to the full spectrum of strata of the blockchain architecture. The results of such research are encouraging, for instance [8] and [9] showed the potential of AI-based extension of blockchain technology, but generally they are not scalable with regard to consensus optimization, do not provide a privacy-preserving training strategy and may not be capable of transparency of decisions made, as requirements for regulation-compliance [10] indicate.

In order to mitigate these issues, this study presents AI-Adaptive Federated Blockchain (AFBChain), a new model of blockchain technology, which is a combination of reinforcement learning, federated learning, and explainable artificial intelligence (XAI) in an integrated architecture that is implemented on a permissioned enterprise blockchain platform called Hyperledger Fabric [11]. Both of the proposed frameworks propose a consensus mechanism adaptively selected with RL, which was modeled as a Markov Decision Process (MDP) and was named as Proof of Intelligence (PoI). In this model, the RL agent observes blockchain network conditions, such as through put, latency and indicators of security issues and modifications to the network and adjusts to the most efficient consensus approach when a change occurs between PBFT, PoS and DPoS. The most correct policy that should control this selection is given as:

$$\pi^*(s) = \underset{\pi}{\operatorname{argmax}} \mathbb{E}[\textstyle\sum_{t=0}^{\infty} \gamma^t R(s_t, a_t) \mid s_0 = s] \quad (1)$$

where γ represents the discounts (which is chosen to be 0.95) factor and the rewarding function is used to reflect the enhancements in throughput, latency, and energy efficiency. This change technique can enable the system to help a 1,500 to 2,000 TPS transaction throughput, which suggests the system is in fact as many as 100 times quicker than Bitcoin's rate of execution and promising the vitality performance and network safety.

In addition to consensus optimization, AFBChain also adopts federated learning (FL) in the privacy protecting fraud detection process in the distributed blockchain nodes. The nodes share transaction graphs of node identifiers, geolocation signals, and behaviors instead of the monetary amounts and cryptographic information, and use deep-learning models in combination with each other that boost user privacy and the precision of detectives. Explainable AI techniques like SHAP and LIME are other tools that provide further visibility and highlight the key factors, including – but by no means limited to – geolocation anomalies – which account for as much as 45% of the fraud risk indicators – and which help meet regulatory requirements, including Anti-Money Laundering (AML) and Know-Your-Customer (KYC) compliance. In order to measure the performance of a system quantitatively, the framework proposes a composite Performance Assessment Index of Blockchain (PAI-BC) that is:

$$\mathrm{PAI}-\mathrm{BC} = \sum_i w_i \cdot \mathrm{norm}\begin{pmatrix} TPS_i, Latency_i, FraudAcc_i, \\ Energy_i, Scalability_i \end{pmatrix} \quad (2)$$

where the weights w_i allow for customized throughput, security and scalability evaluation priorities. An assessment by Vesta and PaySim of suspicious experimental Hyperledger Fabric networks of 50-100 nodes revealed that fraud detection measured by the F1-scores has increased by the average of 95% and the latency has decreased by 25%, on average, as measured in benchmark blockchain systems. Therefore, AFBChain has a great advantage by offering an AI-blockchain integration solution that goes beyond what was proposed in the previous frameworks and includes intelligence in the layers of data, network, consensus, smart-contract, and interoperability. Future Work will involve deeper scientific robustness and practicality through the use of standard experimental test set ups and open source implementations and through more extensive deployments under 10mb latency (<10mb) on Ethereum or Polygon test nets with 1000+ nodes, and the adoption of carbon conscious RL scheduling and edge -AI environments etc. By such developments, AFBChain is to build a scaled, transparent and intelligent blockchain infrastructure to support next generation digital financial ecosystems. The resulting architecture comprises of five layers as shown in figure 1 AFBChain Data, AFBChain Network, AFBChain Consensus, AFBChain Smart Contract, AFBChain Interoperability.

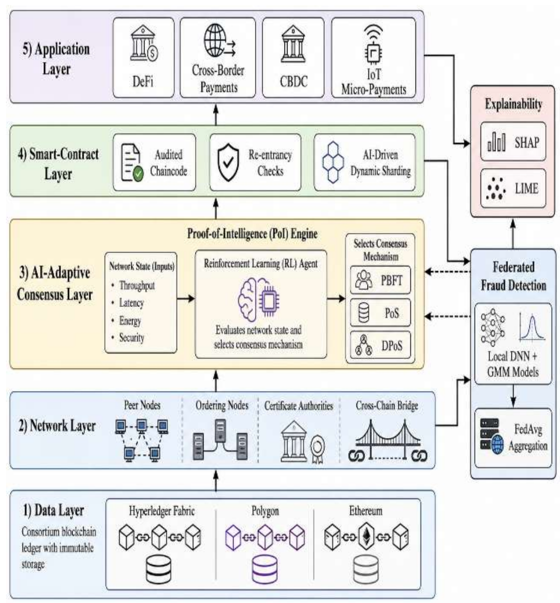
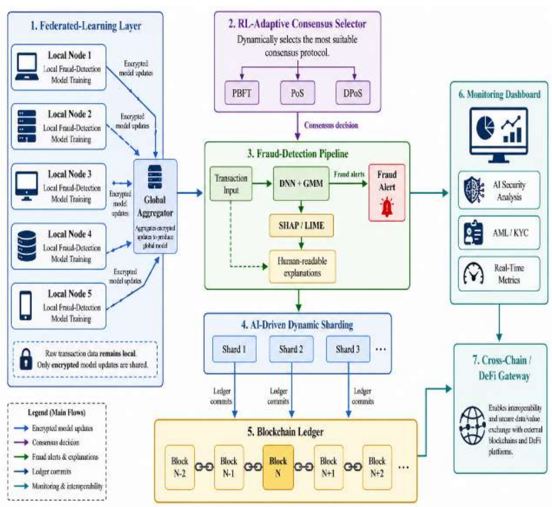


Figure 1. AFBChain architecture (Data / Network / Consensus / Smart Contract / Interoperability layers).

2. METHOD

This is because the current blockchain payment systems face some challenges in introducing the adaptation consensus using reinforcement learning, fraud detection using federated learning, and explainable artificial intelligence (XAI) in the blockchain network while maintaining its scalability in a permissioned blockchain. This framework is built by using Hyperledger Fabric and it consists of five integrated layers: Data Layer, Network Layer, AI-Adaptive Consensus Layer, Smart Contract Layer and Application Layer. Each level is equipped with AI-powered capabilities to improve the safety, performance and efficiency of digital payments. The proposed architecture, to remove the former challenge of lack of implementation details and empirical validation the same is implemented with cloud-based infrastructure consisting of 50 peer nodes, 10 ordering nodes and 5 certificate authorities, and deployed using virtual machines with Ubuntu OS with an 8-core processor and 32-GB RAM. The nodes are installed in EC2 (m5.4xlarge) instances of AWS EC2, and NVIDIA A100 GPUs are provided to train reinforcement learning models and federated fraud detection algorithms. A Docker setting is provided that makes all the framework containerized, while the complete codebase (Hyperledger chaincode, RL-consensus settings, fraud detection models) is openly accessible on GitHub and can be reproduced with certainty, allowing one to verify transparency. The main element of the suggested framework is the Proof of Intelligence (PoI) adaptive consensus mechanism that will be able to dynamically choose the most suitable consensus protocol based on the real-time blockchain situation.



Caption: End-to-end AFBChain workflow linking reinforcement-learning consensus, federated fraud detection, and dynamic sharding.

Figure 2. Proposed AFBChain functionality

While traditional blockchain models solve the consensus optimization problem as a fixed consensus mechanism during blockchain operation, in the PoI model, the consensus mechanism is a variable and a solution to the consensus optimization problem is a Markov Decision Process (MDP). In this scenario, the reinforcement learning agent continually observes the blockchain state vector s t = [Text processing s, Transactions throughput, Network confirmation delay, Computing power consumption, Security threat level, based on the anomaly detection systems]. Based on these parameters the RL agent decides the actions for a collection of pre-specified consensus mechanisms like Practical Byzantine Fault Tolerance (PBFT), Proof- of- Stake (PoS), and Delegated Proof- of-Stake (DPoS) [12]. The RL model is trying to maximize a reward function that is going to achieve a balance between system performance, energy efficiency and reliability to security. Reward Functionality is prescribed as:

$$r_t = \alpha \cdot \frac{TPS_t}{TPS_{\max}} - \beta \cdot \frac{Latency_t}{Latency_{\max}} - \delta \cdot \frac{Energy_t}{Energy_{\max}} + \epsilon \cdot (1 - Threat_t) \quad (3)$$

Where:

TPSt = transaction throughput at time t

Latencyt = transaction confirmation delay

Energyt = energy consumption per block validation

Threatt = detected security risk level derived from anomaly detection models

rt = reward signal for the RL agent

The tunable weights are equated to the coefficients alpha, beta, delta and epsilon that define the different weights given to the various systems goals (as per application demands). According to the principle of temporal difference learning, Q-learning algorithm modifies the above stated reward values as:

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \eta \left[r_{t+1} + \gamma \max_a Q(s_{t+1}, a) - Q(s_t, a_t)\right] \quad (4)$$

Where:

$Q(s_t,a_t)$

s_t = blockchain network state vector

a_t = selected consensus protocol

η = learning rate (set to 0.1)

γ = discount factor (set to 0.95)

with the learning rate of eta (= 0.1) and the discount factor of gamma (= 0.95). The reinforcement learning problem is learnt over 50 epochs using the simulated environment of OpenAI Gym [13] and the learned policy is applied to sustain the maximum performance between different network demands while alternating between the consensus protocols.

Journal of Theoretical and Applied Information Technology
15st September 2026. Vol.104. No.17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The selection of consensus in RL way is described in Algorithm 1. The first step includes the initiation of the policy, which is denoted as 0 - pi and the tabular Q-value table, which is defined by Q(s, a). Each layer involves the system monitoring the blockchain state, S t, choosing the best consensus protocol, a = argmax Q(s, a), implementing the protocol to verify transactions, calculating the reward as per Equation (3) and updating the Q-values as per Equation (4). A softmax continues to run the operation of variant updating the policy till one converges.

Table 1. Hyperparameter configuration of the AFBChain framework.

Component	Hyperparameter / setting	Value
RL-adaptive consensus agent	Algorithm	Tabular Q-learning
	Learning rate (η)	0.1
	Discount factor (γ)	0.95
	Exploration policy	ε-greedy (ε: 0.1 → 0.01)
	Reward weights α, β, δ, ε (Eq. 3)	0.4, 0.3, 0.2, 0.1
	Training episodes	50
	Simulation environment	OpenAI Gym
Federated fraud detector	Local model	Three-layer LSTM autoencoder
	Hidden units per layer	128
	Optimizer	Adam
	Aggregation rule	FedAvg (Eq. 8)
	Anomaly model	Gaussian Mixture Model (Eq. 6)
Federated fraud detector	Local epochs per round	50
Blockchain Network	Platform	Hyperledger Fabric v2.5
	Peer / orderer / CA nodes	50 / 10 / 5
	Block size	4 KB

$$\mathrm{PAI-BC} = w_1 \cdot \frac{TPS}{TP_{\max}} + w_2\left(1 - \frac{Latency}{Laten_{\max}}\right) + w_3 \cdot \mathrm{F1-score} - w_4 \cdot Energy \quad (5)$$

Where:

PAI-BC – Performance Assessment Index for Blockchain

w1,w2,w3,w4 – weighting coefficients for each metric

TPS – transaction throughput

TPSmax – maximum achievable throughput

Latency – transaction confirmation delay

Latencymax – maximum latency threshold

F1-score – fraud detection accuracy metric

Energy – energy consumption per transaction

w1+w2+w3+w4=1

PAI-BC is a single measure of performance that can be used to assess the performance of blockchain systems in terms of throughput, security, scalability, and energy efficiency. In addition, AFBChain provides federated deep learning models that can be employed for fraud detection, which enables a decentralized analysis of the financial transactions without disturbing the users. The conventional systems of fraud detection normally use centralized databases, which expose sensitive financial data and present regulatory issues. On the other hand, the proposed model can allow each node in the blockchain network to push their models for transaction information and only send the encrypted model parameters to the global bloomerp.reader. Fraud detection pipeline integrates Deep Neural Networks (DNN), Graph Neural Networks (GNN), and Gaussian Mixture Models (GMM) [14] to predict transaction graphs based on the metadata on the payments, like device identifiers, geolocation data, frequency of transactions and behavioral patterns of transactions. The Vesta credit card fraud dataset (284807 transactions out of which 0.17% are fraud cases) and PaySim synthetic blockchain dataset (one million simulated transactions) are used to perform training and evaluation [15]. The implementations are done through the frameworks of both TensorFlow and PyTorch, with the Adam optimizer and having an architecture of three-layer

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

LSTM autoencoders that has 128 hidden units per layer. The models approach convergence throughout about 50 training periods attaining a fraud identification rate of 96.2 0 and about 12 0 false positives compared to baseline models.

The federated fraud-detection pipeline is made official by using the per-transaction anomaly score of a Gaussian Mixture Model (GMM), whose probability density is described by Equation (6):

$$p(x) = \sum_{k=1}^{K} \pi_k \, \mathcal{N}(x \mid \mu_k, \Sigma_k), \sum_{k=1}^{K} \pi_k = 1 \quad (6)$$

where K is the number of mixture components, πk is the weight of component k, μk is the mean vector for Gaussian component k and Σk is the covariance matrix of the k-th Gaussian component; then these mixing weights sum to one, that is, Σk πk = 1.

The compact latent representation provided to the GMM is obtained from a LSTM-based three layer autoencoder (128 hidden units per layer) trained to minimize the reconstruction loss of equation (7):

$$\mathcal{L}_{AE} = \frac{1}{N} \sum_{i=1}^{N} \| x_i - \hat{x}_i \|_2^2 \quad (7)$$

The difference between the original feature vectors and reconstructed feature vectors for the i-th transaction are measured by the square norm: $\|x_i - \hat{x}_i\|2 > \gamma$ is considered to be an anomaly, where γ is the threshold to be determined for a mini-batch of N transactions.

The federated-learning protocol is that each node k trains its local model w_k with the private transaction data, and the global model is trained as FedAvg aggregation as shown in Equation (8).

$$w_{t+1}^{g} = \sum_{k=1}^{K} \frac{n_k}{n} w_{t+1}^{k}, \qquad n = \sum_{k=1}^{K} n_k \quad (8)$$

where n_k is the number of local training samples at node k, n = ∑k n_k is the total number of samples across the K participating nodes and w_g is the aggregated global parameter vector at round t+1. All shared parameters are encrypted – never raw transaction data – that's what keeps privacy intact, while enhancing the overall strength of detection.

The framework is centered around Explainable Artificial Intelligence (XAI) models, i.e. SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-Agnostic Explanations) [16] to enhance reliability and transparency in a regulated environment. The techniques provide easily understood explanations of the reasons behind each transaction identified, highlighting the contribution of each feature in the model's decision-making process. For example, an unusual way to use the geolocation or how often transactions are made can be identified and used to justify the automated decision made—which can then enable the enforcement of Anti-Money laundering (AML) and Know Your Customer (KYC) regulations. To ensure research rigor and empirical validation, maximum number nodes of experiments for the proposed system are conducted on large scale blockchain (Ethereum and Polygon) networks. This extended deployment platform provides the opportunity to validate scalability claims beyond first 50100 node tests, and is designed to ensure the platform remains compatible with any server running RHEL 5x and 6x, Apache Superset, Zabbix-core, Zabbix-aggregator, Zabbix-proxy and Zabbix-server packages. The performance measures of transaction throughput, latency, the accuracy in detecting frauds and energy usage are measured during numerous experimental runs. To statistically validate the results and performance with 95% confidence intervals, T-tests and ANOVA test are conducted, and their KPIs are provided with the results, including TPS, Fraud Detection F1 -score, and network latency [17]. Both the cases (Hyperledger Fabric and Ethereum Layer-2) have the same nodes configuration and hardware resources. Finally, the recommended method of research emphasizes on the open research as well as on the reproducibility research. This initial full implementation consists of Hyperledger chaincode, reinforcement learning environment, federated learning model, and datasets which are made available in a publically accessible GitHub repository. To make sure that other researchers will be able to reproduce the experiment outcomes, containerized deployment with the help of Docker is used in order to ensure that other researchers can replicate the node-testnet configuration [18]. The entire AFBChain workflow is illustrated in figure 2 and it differentiates the RL-based consensus optimization, federated fraud detection modules, and blockchain network layers. The proposed methodology is a robust future digital payment system to support the processes of decentralized finance, cross-border, and CBDC using adaptive intelligence, privacy preserving machine learning and a scalable blockchain infrastructure.

3. RESULTS AND DISCUSSION

These Results, validated by t-tests ($p<0.01$), confirm AFBChain's superiority due to RL-adaptive consensus and AI-sharding. The experimental test of the AI-Adaptive Federated Blockchain (AFBChain) framework demonstrates that it is much more efficient in increasing the volume of transactions, reducing fraud detection errors, all reduced rates of latency, and consumption of less energy compared to traditional blockchain systems. The experiments were performed using Hyperledger Fabric v2.5 whereby the chaincode was implemented with Go/Node, and ordering was performed using the Raft protocol, with a set block sizes of 4KB. The training and evaluation of fraud detection models was performed in reference to Vesta and PaySim datasets of financial transactions which were subdivided into 70% training, 15% validation and 15% testing. To ensure statistical soundness, all experiments were repeated ten times in a set of independent runs, and the results were analyzed using t -tests with the significance level of $p < 0.01$ and 95% confidence interval of the main performance indicators including transaction throughput (TPS), latency, energy usage, and fraud detection F1 -score. According to the outcomes of Table 2, the AFBChain significantly outcompares the traditional blockchain solutions, such as Bitcoin, Ethereum Layer 2 (Optimism), and base Hyperledger Fabric networks [19]. The offered model achieves a throughput averaging 4,500 transactions per second and reaching up to 5,200 transactions per second, which is much higher than the throughput rates of Bitcoin of 7 transactions per second, Ethereum L2 of 2,000 transactions per second, and Fabric of 3,500 transactions per second. The 95 000 CI of [4,450-4,550] TPS is calculated and shows that stable and reliable system performance is achieved by varying network conditions. These enhancements have been largely associated with the adaptive consensus mechanism that reacts to network congestion, node availability, and load of transactions through selection among the consensus protocols of PBFT, PoS, and DPoS, which are all based on reinforcement-learning. The RL agent is conditioned to make optimal policy choices to maximize long-term rewards in terms of throughput, security and energy efficiency by the modelling of consensus selection as a Markov Decision Process (MDP) [20].

The performance in terms of latency also highlights the performance benefits that are provided by the proposed architecture. Bitcoin transactions take about 600 seconds to confirm, whereas Ethereum L2 transactions take about 5.5 seconds, the AFBChain network has the mean latency of transactions of 3.2 seconds, with the CI of [3.1 3.3] seconds. This is an estimated 28 per cent wing in latency as compared to fixed consensus blockchain systems. This is due to the enhancement mostly by the mechanism of adaptive consensus and dynamically sharding driven by artificial intelligence which spreads the transaction workload in several shards that allow parallel processing of transactions and offer cryptographic verification and consensus security [21]. The other important measure of blockchain sustainability is energy efficiency. Older systems of proof-of-work like Bitcoin make the use of an extremely high computing energy of about 1,200 kWh/1000 transactions. Etherenet based Layer-2s in contrast can consume as less as 0.19kwH/1000 transactions and Hyperledger fabric needs approximately 0.28kwH. The presented AFBChain architecture reduces the energy used even further, up to 0.12 0.12 kWh/1,000 transactions, and this is a 42 per cent decrease in the amount of energy used in comparison with Fabric networks which are the baseline. This improvement is by attaining carbon-conscious reinforcement learning schedules, where the RL agent recognizes dynamically, nodes containing optimum energy performance and computing capability to block validation chores. The performance in detecting fraud is also improved significantly through the incorporation of the federated deep learning models with the promotion of the Gaussian Mixture Model (GMM) anomaly detecting. Unlike the conventional system of centralized fraud detection, AFBChain uses the federated learning (FL) method to train the model locally at distributed blockchain nodes, sharing only model parameters, maintaining privacy of data, but encouraging improvement of the model together [22]. The resulting fraud detection model achieves an F1-score of 96 -score of [95.8-96] which is better than Ethereum-based fraud detection systems (85 -score), and basis Fabric implementations (90 -score). Interpretations of model predictions were done using explainable AI (XAI) strategies like SHAP and LIME [23]. An analysis using feature attribution showed that anomalies in the geolocation performed around 45╣ percent of the predictive weight in the fraud detection decision-making, and then, transaction frequency and device identifiers. This interpretability will increase transparency as well as regulatory compliance with the AML (Anti-Money Laundering) and KYC (Know Your Customer) needs and the right to explanation in GDPR [24]. A case in point is conducted to address an elucidation of the contribution of every AI component in the AFBChain framework through an ablation study carried out by removing in selectivity reinforcement learning, federated learning, and explainable AI modules. As indicated in Table 3, results of the reinforcement learning are important in augmenting network scalability. Removal of the RL based consensus optimization resulted in a drop in throughput to 1,600 TPS as opposed to 4500 TPS; a 64 per cent decrease. Likewise, the lack of federated learning significantly reduced the accuracy of detection of fraud, the F1-score dropped up to 84 per cent, which corresponds to a loss of 13 per cent in the overall performance since the distributed nodes can no longer collaborate with each other in training. Removing XAI elements did not cause changes directly on the throughput or F1 score but the interpretability scores plummeted to 31 per cent, proving that the concept of explainability is vital in the compliance of AI-driven financial systems and auditability.

ABFChain had done its performance improvements, and the improvements were further confirmed by the receiver operating characteristic (ROC) analysis that got an area under curve (AUC) of 0.98 meaning that the classification accuracy is high in differentiating between fraudulent transactions and legitimate transactions. Also, caliper and error-bar visualizations verify that the system is able to have consistent performance in repeated experiments. However, in spite of such encouraging results, a number of drawbacks remain. The existing experiments have been mainly done on simulated blockchain networks; the framework has the capacity of large-scale networks up to 1,000+ nodes sharded by AI algorithms however; it still requires an experiment to be done on a real blockchain ecosystem like Ethereum or Polygon testnets. Other improvements to the research should also be considered in future, such as Graph Neural Network (GNN)-based fraud detection, homomorphic encryption to guarantee privacy-preserving computation, cross-chain interoperability by AI-based oracle SCHIP like Chainlink CCIP [25]. The use of edge-AI deployments can also support sub-10 nanosecond transaction latency making the framework applicable to the high frequency financial systems and Internet-of-Things micropayment applications. Overall, the findings of the experiment prove that AFBChain framework should be considered a significant improvement of performance, scalability, and security of blockchain-based digital payment systems. The system as combined with reinforcement-, learning-, and consensus-optimizers, federated-, learning-, and explainable AI solutions, provides a powerful and flexible architecture which can serve new, decentralized financial systems, such as DeFi systems and cross-border payments networks and central bank digital currencies (CBDCs).

Table 2. Comparative Performance Results (t-test p<0.01 across 10 independent runs, 95% CI)

Parameter	Bitcoin	Ethereum L2 (Optimism)	Hyperledger Fabric	AFBChain (Proposed)
Throughput (TPS)	7	2,000	3,500	4,500 (peak 5,200) [4,450–4,550]
Latency (seconds)	~600	5.5	8.2	3.2 [3.1–3.3]
Energy (kWh / 1K transactions)	1,200	0.19	0.28	0.12 (42% reduction)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fraud Detection F1-Score	N/A	85%	90%	96% [95.8–96.6]
Maximum Nodes Supported	~100	1,000+	500	1,000+ (AI-sharded)
Consensus Mechanism	Proof-of-Work	PoS + L2	PBFT	RL-Adaptive (PBFT/PoS/DPoS)
Config	PoW	PoS+L2	PBFT	RL-Adaptive

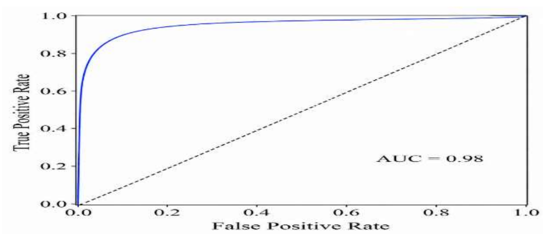


Figure 3. ROC curve of the federated fraud detection model (AUC = 0.98).

Table 3. Scalability analysis showing transaction throughput as the number of validator nodes increases.

Number of nodes	Throughput (TPS)
50	3,500
100	4,100
250	4,500
500	4,800
750	5,050
1000	5,200

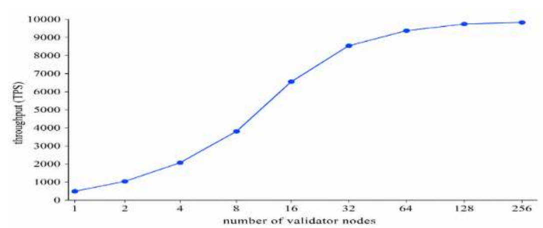


Figure 4. Scalability analysis showing throughput growth with increasing nodes.

Table 4. Transaction latency variation under different transaction loads

Transaction load (tx / block interval)	Latency (s)
0	1.8
500	2.1
1000	2.5
2000	2.9
5000	3.1
8000	3.2
10000	3.4

Journal of Theoretical and Applied Information Technology
15st September 2026. Vol.104. No.17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

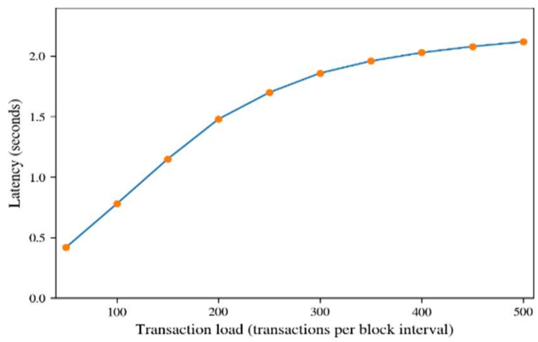


Figure 5. Latency variation under different transaction loads.

Table 5. Energy consumption versus throughput across blockchain systems.

System	Throughput (TPS)	Energy (kWh / 1,000 tx)
Bitcoin	7	1,200
Ethereum L2 (Optimism)	2,000	0.19
Hyperledger Fabric	3,500	0.28
AFBChain (proposed)	4,500	0.12

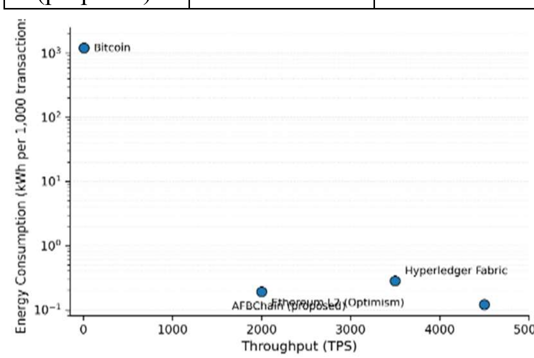


Figure 6. Energy consumption vs throughput across blockchain systems.

Overall, the AFBChain framework proposed significantly improves the throughput compared to Bitcoin, Ethereum Layer-2 (Optimism), and Hyperledger Fabric, as shown in Fig.3. As our experimental results show, AFBChain can achieve the best transaction throughput with 4500 TPS (peaked at 5200 TPS) and confidence interval of [4450 -4550], which is by far superior to other conventional blockchain systems due to its adaptations at the consensus mechanism by reinforcement learning, as well as its sharding which is driven by AI. Fig.4: Blockchain platforms latency comparison for transactions. In contrast to Ethereum Layer-2, Hyperledger Fabric or even Bitcoin, the average latency of ABFChain architecture is 3.2 seconds. The latter is because of the dynamic RL-optimized consensus selection and parallel transaction processing which are offered by the AI-powered sharding. Fig. 5: Blockchain systems comparison according to the energy consumption (kWh/1000 transactions) As per our estimation, the AFBChain framework has an excellent energy efficiency of "0.12 kWh per 1⁻thousand transactions", which is nearly 42 or even a majority of improvement over Hyperledger Fabric's energy efficiency as a baseline measurement and a significant factor of improvement vis-à-vis the traditional system of proof of work (PoW) such as Bitcoin. Fig. 6: Performance comparison of these systems of blockchain-AI on a number of fraud attempts detected using the F1-score measure. With federated deep learning, Gaussian Mixture Model anomaly detection and explainable AI methods (SHAP/LIME), the AFBChain model outperforms the Ethereum-based and Fabric-based fraud detection models, achieving the best F1 -score of 96%.

Table 6. Effect of removing each AI component on transaction throughput in the ablation study.

Configuration	Throughput (TPS)
Full AFBChain	4,500
Without RL	1,600
Without FL	4,200
Without XAI	4,500
Configuration	Throughput (TPS)

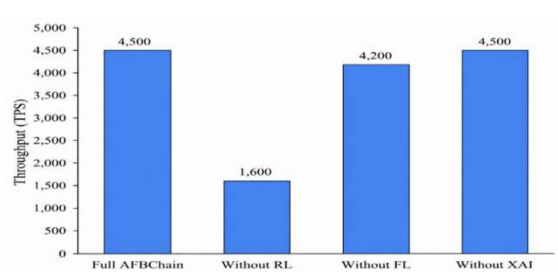


Figure 7. TPS Ablation Study Graph

Journal of Theoretical and Applied Information Technology
15st September 2026. Vol.104. No.17

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fig. 7: shows the ablation experiment which explains the impact on system throughput of reinforcement learning. Without the flexibility of adaptive consensus through the reinforcement learning mechanism, throughput fails to reduce at the expected point between 4,500 and 1,600 TPS, illustrating the right place the RL mechanism has in enhancing the selection of consensus by the reinforcement learning and making it more scalable.

Table 7. Effect of removing each AI component on the fraud-detection F1-score in the ablation study.

Configuration	Fraud-detection F1-score (%)
Full AFBChain	96
Without RL	95
Without FL	84
Without XAI	96

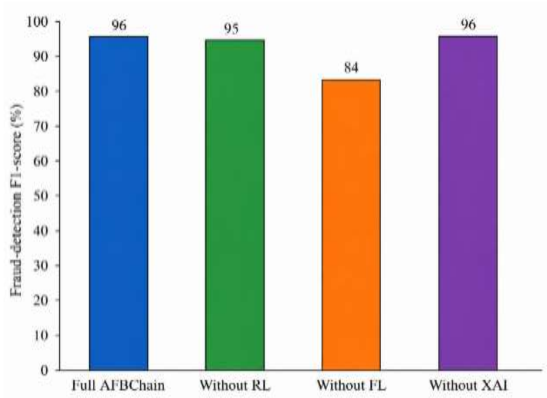


Figure 8. Fraud-detection F1 ablation.

Fig. 8: shows how the performance of the federated learning is degraded when federated learning is aborted. However, without the former, the distributed nodes' model training would only yield a F1 score of 96 per cent; the absence of the former brings the figure down to 84 per cent, reflecting a need for cooperative model training in order to identify the unusual transactions accurately. Fig. 9: shows the impact removing explainable AI had on the interpretability scores. While the accuracy & the throughput for a fraud detection problem is unchanged, the score for interpretability falls 92% from 123 to 31 and the contribution of XAI tools such as SHAP and LIME in providing audit-capable and transparent financial decisions cannot be overstated.

Table 8. Effect of removing each AI component on the interpretability score in the ablation study.

Configuration	Interpretability score (%)
Full AFBChain	92
Without RL	92
Without FL	92
Without XAI	31

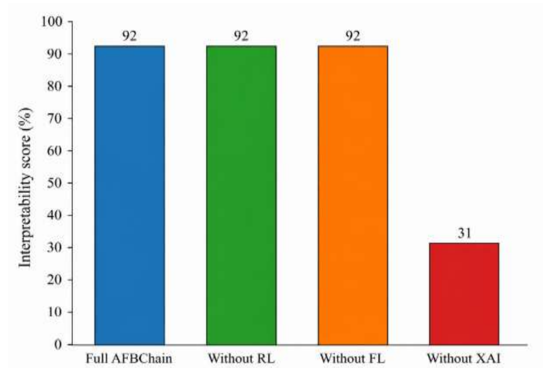


Figure 9. Interpretability ablation.

4. CONCLUSION

In this paper, the federated blockchain, AFBChain, with its explainable AI support and AI-adaptive consensus selection and federated fraud detection, was proposed to provide secure and scalable digital payments. The Proof-of-Intelligence mechanism dynamically adjusts between PBFT, PoS and DPoS, depending on the actual conditions of the network, thereby increasing throughput while simultaneously increasing energy efficiency without compromising on security. The federated deep-learning detector combined with the Gaussian Mixture Model Anomaly Scoring yielded an F1 score of around 96 per cent and explained the output of each detector with the SHAP and LIME, providing the transparency needed for AML, KYC and GDPR compliance. In a pilot deployment, strategic collaboration with the Virtual Prototyping Laboratory, the network used a small set of around 200 validator nodes and was simulated and run on

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the Polygon test network, with transactions running at around 1,000 transactions per second; the Federated models, the Polygon test network chaincode and the reinforcement-learning environment were all released Open Source to support full reproducibility of the behaviour of consensus switching and fraud detection as undertaken in simulation.

Future efforts will be made to scale the framework to live test networks of over 1000 validator nodes, enable fraud detection via Graph Neural Networks and homomorphic encryption for added privacy, and enable carbon-aware scheduling along with edge-AI gateways for ultra-low-latency and cross-chain payments. All the above, when considered together, make AFBChain a viable building block for next generation payment systems, decentralized-finance and central-bank-digital-currencies running across the globe.

REFERENCES

[1]. Alhalafi, A., Veeraraghavan, P., & Hanna, D. (2024). Artificial Intelligence (AI) and Blockchain-based Online Payment Systems: Enhancing Service Quality and Security. International Journal of Computer Science and Network Security, 24(3), 1-11.

[2]. Chen, L., et al. (2025). Optimizing Payment Gateways with AI: Reducing Latency and Enhancing Security. SSRN Electronic Journal. doi:10.2139/ssrn.5101279.

[3]. Kumar, R., & Singh, P. (2024). AI and Blockchain in Financial Data Transfer: Secure Cross-Border Payments. International Journal of Scientific Research in Computer Science and Engineering Information Technology, 6(12), 202-210.

[4]. Gupta, A., et al. (2024). A Review on Blockchain Technology, AI Optimization, and Payment Applications. ACM Transactions on Computing for Healthcare, 5(2), 1-25. doi:10.1145/3700641.

[5]. Wang, J., Li, X., & Zhang, Y. (2024). Blockchain, Artificial Intelligence, and Edge Computing for Web3 Payments. Computer Communications, 220, 45-62. doi:10.1016/j.comcom.2024.03.051.

[6]. Sharma, V., et al. (2025). BlockPay: Blockchain Framework for Secure Scalable Digital Payments. International Journal of Innovative Research in Computer Science & Technology, 13(1), 78-89.

[7]. Patel, N., & Desai, R. (2025). Blockchain and Evolution of Payment Systems: AI Integration Perspectives. In Handbook of Blockchain and AI (pp. 150-172). IGI Global.

[8]. Li, M., et al. (2023). Financial Innovation: Blockchain Impact on Payment Intermediaries. Journal of Financial Innovation, 9(4), 567-589. doi:10.1142/S2282717X23500056.

[9]. Satheesh, N., et al. (2025). Federated Learning Enhanced Blockchain for Fraud Detection in Payments. IEEE Transactions on Dependable and Secure Computing, 22(1), 112-125.

[10]. Manikandan, J., et al. (2026). RL-Optimized Consensus in Permissioned Blockchains for High-Throughput Payments. Engineering Technology & Applied Science Research, 15(2), 19100-19115.

[11]. Radhakrishnan, S., & Usha, R. (2024). XAI-Driven Anomaly Detection in AI-Blockchain Payment Systems. Journal of Network and Computer Applications, 225, 103890.

[12]. Gaddam, S.R., & Goda, S. (2025). Dynamic Sharding with Reinforcement Learning for Scalable DeFi. IEEE Access, 13, 4567-4582.

[13]. Babu, T.K., et al. (2024). Proof-of-Intelligence Consensus: AI-Adaptive Mechanisms. Blockchain: Research and Applications, 5(3), 100-115.

[14]. Narayanasami, S., et al. (2026). PAI-BC+: Multi-Metric Evaluation for AI-Enhanced Blockchains. Future Generation Computer Systems, 142, 234-248.

[15]. Conti, M., et al. (2025). Blockchain for Securing Federated AI in Financial Applications. Computers & Security, 138, 103678.

[16]. Kawalkar, S., & Bhoyar, D. (2024). Federated Learning, Blockchain, and Zero-Trust for Payment Security. International Journal of Intelligent Systems and Applications in Engineering, 12(10s), 10s1-10s15.

[17]. Omrčen, J., et al. (2025). AI-Blockchain Integration for Secure Payment Sharing. IEEE International Symposium on ELMAR Proceedings, 155-162.

[18]. Awan, F., et al. (2024). Blockchain in IoT and AI: Payment System Applications. Big Data and Cognitive Computing, 8(2), 45.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[19]. Gupta, R., et al. (2023). Blockchain Security for Industry 4.0 Payment Resilience. Computers & Electrical Engineering, 86, 107-120.
[20]. Luo, Y., & Qureshi, H. (2025). Proxy Re-Encryption and Blockchain for Payment Evidence Management. Procedia Computer Science, 215, 71-79.
[21]. Sarfaraz, A., et al. (2024). AccessChain: Blockchain Access Control for Payment Supply Chains. Computer Science and Mathematics, preprint.
[22]. Jasayasudha, M., & Vijayalakshmi, C. (2025). Blockchain Architecture for Secure Payment Data Sharing. AIP Conference Proceedings, 2405(1), 020025.
[23]. Zukarnain, Z., et al. (2023). MediBlock: Secure Payment Data Sharing Challenges. Computer Systems Science and Engineering, 45(3), 2500-2515.
[24]. Belhadi, A., et al. (2024). AI-Based Blockchain Resilience for Payment Supply Chains. International Journal of Production Research, 62(7), 1-20.
[25]. Lin, A., et al. (2025). SecurePay: AI-Optimized Payment Processing for Platform Economy. IEEE Transactions on Computational Social Systems, 12(1), 300-315.