OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

BLOCKCHAIN- ASSISTED AI FRAMEWORK FOR SECURE ONLINE TRANSACTIONS AND FRAUD INTELLIGENCE

KHAN EBTESAM AFROZ[1],DR. V. S. KARWANDE[2],ASST. PROF. A. A. KHAN[3]

M.Tech Student, Computer Science and Engineering Department, Everest College of engineering and technology, chhatrapati Sambhajinagar[1]

HOD, Computer Science and Engineering Department, Everest College of engineering and technology, chhatrapati Sambhajinagar[2]

Prof, Computer Science and Engineering Department, Everest College of engineering and technology, chhatrapati Sambhajinagar[3]

Abstract: ***The rapid digitalization of financial systems has led to an exponential rise in electronic transactions—and a corresponding escalation in sophisticated online fraud. Traditional machine-learning models, while effective at identifying anomalous behavior, suffer from low interpretability, mutable evidence logs, and difficulty in maintaining integrity during dispute investigations. This paper proposes an AI-led blockchain-based framework designed to achieve high-recall fraud detection, explainable decision reasoning, and tamper-proof evidence management. The architecture integrates a cost-sensitive ensemble model for rare-event detection, an explainable AI layer for transparent reasoning, and a permissioned blockchain ledger for immutable evidence anchoring and dispute-resolution tracking. Performance targets emphasize sub-second real-time processing and verifiable audit trails that meet regulatory expectations for accountability and transparency. The proposed framework aims to advance payment-integrity assurance by combining the predictive power of artificial intelligence with the trust guarantees of blockchain technology.***

Keywords: Artificial Intelligence, Blockchain, Fraud Detection, Explainable AI, Financial Transactions, Payment Integrity, Tamper-Proof Evidence, Real-Time Analytics

---

I. INTRODUCTION

The global expansion of e-commerce, digital banking, and realtime payment systems has significantly increased both the volume and velocity of financial transactions. Alongside this growth, online fraud has evolved into a major security and economic concern. Sophisticated threats—such as identity theft, synthetic account creation, card-not-present (CNP) fraud, and deepfakebased impersonation—continue to challenge the reliability of current fraud detection mechanisms. According to industry analyses, financial institutions lose billions annually to fraudulent activities, despite deploying various machine-learning and rulebased systems. The increasing complexity of fraud patterns, the speed of transactions, and the requirement for regulatory transparency demand a more resilient and explainable approach to payment integrity.

Traditional fraud detection systems primarily rely on rule-based filters or conventional classifiers trained on historical data. While these systems perform adequately for known fraud scenarios, they fail to generalize to emerging patterns and adversarial behaviors. Moreover, the inherent class imbalance in transactional datasets—where genuine transactions vastly outnumber fraudulent ones—causes models to favor precision over recall, thereby missing critical fraud events. Furthermore, the absence of interpretability and verifiable logging mechanisms limits the ability of financial organizations to justify model decisions during dispute resolution or regulatory audits. Consequently, the financial sector faces a dual challenge: developing intelligent systems that can detect rare fraud events with high accuracy and ensuring that their operations remain transparent, auditable, and tamper-proof.

Artificial Intelligence (AI) and Blockchain technologies together offer a promising direction to overcome these limitations. AIdriven models provide adaptive, data-driven learning capabilities for real-time fraud prediction, while blockchain introduces immutable data integrity and verifiable evidence management. By combining these technologies, it becomes possible to design an integrated fraud detection framework that delivers both predictive accuracy and operational trust. The AI component contributes to the detection of anomalous patterns using cost-sensitive learning and explainable reasoning, whereas the blockchain layer ensures secure storage of audit trails and supports transparent dispute workflows.

This paper presents an AI-led blockchain framework that enhances fraud detection and payment integrity in online transactions. The proposed approach integrates a high-recall ensemble detection model, an explainable AI module for interpretability, and a

permissioned blockchain for immutable evidence anchoring and traceability. By incorporating data-drift monitoring, structured dispute handling, and sub-second response capabilities, the framework aims to establish a new standard for accountable and transparent financial analytics. The subsequent sections detail the supporting literature, defined problem statement, system objectives, and architectural design of the proposed solution.

II LITERATURE SURVEY

Online financial transactions have become a critical target for fraudulent activities, creating an urgent need for intelligent detection mechanisms. Studies highlight that the inherent class imbalance and adversarial nature of fraud data pose severe challenges for predictive models [1]. Traditional rule-based systems fail to generalize as attackers adapt their behavior, while machine-learning methods require continuous retraining and monitoring to remain effective [2]. Researchers emphasize that conventional accuracy metrics are misleading in rare-event scenarios, suggesting the use of precision–recall AUC and recall at fixed false-positive rates (FPR) as more reliable performance indicators [3].

Machine learning (ML) techniques such as cost-sensitive learning, threshold tuning, and ensemble approaches have shown improved robustness in detecting minority-class fraud patterns [4]. In particular, boosting and stacking ensembles achieve superior performance by combining multiple base models, thereby mitigating overfitting and improving recall under imbalance [5]. Temporal and behavioral features—such as device identifiers, merchant categories, and transaction velocity—have also been integrated into detection models to identify dynamic and contextual anomalies in real time [6].

However, these high-performing models often act as black boxes, offering limited transparency for auditors and regulators. To address this, Explainable Artificial Intelligence (XAI) frameworks have emerged to interpret decision boundaries and provide per-instance explanations for model outputs [7]. Techniques like LIME, SHAP, and counterfactual reasoning enhance trust and accountability by generating reason codes and human-readable narratives for each prediction [8]. This interpretability not only improves user confidence but also supports dispute-resolution workflows and compliance with financial audit standards [9].

Parallelly, blockchain technology has gained attention for its ability to ensure data immutability, traceability, and integrity within financial ecosystems [10]. Permissioned blockchain systems, such as Hyperledger Fabric, allow secure anchoring of evidence hashes, creating verifiable and tamper-proof audit trails [11]. Research further demonstrates that blockchain-enabled smart contracts can automate transaction verification and dispute lifecycle management, enhancing operational transparency [12]. This combination of AI-driven analytics and blockchain-based data integrity forms the foundation for modern, trustworthy fraud detection systems capable of meeting regulatory and performance expectations [13], [14].

III PROBLEM STATEMENT

The exponential growth of online financial transactions has led to an increase in sophisticated fraudulent activities, including identity theft, account takeovers, card-not-present (CNP) fraud, and synthetic identity attacks. Despite the deployment of advanced machine learning and rule-based systems, current fraud detection frameworks continue to face critical limitations in accuracy, transparency, and evidence integrity. Most AI-driven fraud detection models operate as black boxes, offering minimal interpretability for auditors and regulators. Additionally, traditional databases fail to provide immutable records of detected anomalies or disputed transactions, leading to weak traceability and difficulties in forensic validation.

Moreover, the class imbalance inherent in fraud datasets causes a disproportionate bias toward legitimate transactions, resulting in missed fraudulent events with high financial impact. Regulatory requirements now demand explainable decision-making and verifiable audit trails for all high-risk financial operations. However, existing systems lack a unified mechanism that ensures both real-time high-recall fraud detection and tamper-proof evidence management. Therefore, there is an urgent need for an AI-led blockchain framework that integrates detection, interpretability, and immutable evidence anchoring within a single secure architecture to enhance payment integrity and trust in digital transactions.

IV OBJECTIVES

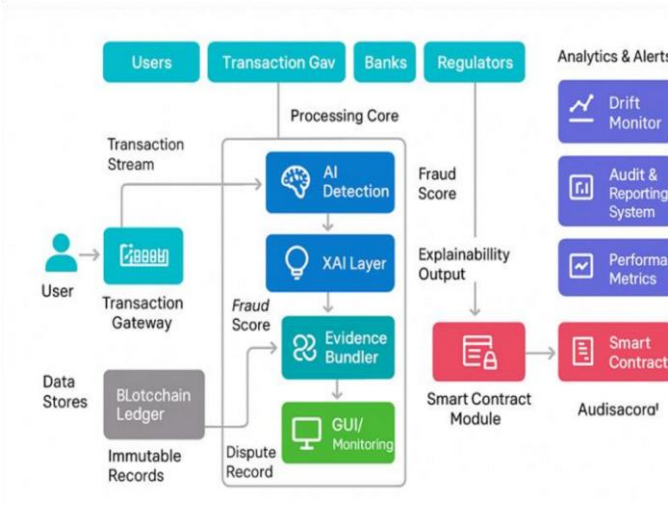
The primary objective of this research is to design and develop an AI-led blockchain framework for ensuring fraud detection and payment integrity in online transactions. The system aims to combine high-recall artificial intelligence models with explainable reasoning and tamper-proof blockchain evidence management.

The specific objectives of the proposed framework are as follows:

1. To develop a high-recall fraud detection model capable of handling severe class imbalance in online transaction datasets.
2. To integrate an Explainable AI (XAI) layer that generates interpretable reason codes for each fraud decision to enhance transparency and trust.
3. To design a tamper-proof evidence management mechanism that securely bundles model decisions and relevant metadata.
4. To establish an immutable audit trail and dispute-resolution workflow using a permissioned blockchain network.
5. To implement a data-drift monitoring module that continuously evaluates feature distribution changes to maintain model reliability.

6. To develop a user-friendly graphical interface (GUI) for real-time fraud visualization, analyst review, and auditing.
7. To ensure end-to-end system performance with transaction processing latency under 0.25 seconds for at least 95% of total operations.

V. SYSTEM ARCHITECTURE



8.

1.Data & Features: Ingest transactional streams (amount, merchant, device/IP, geo, velocity). Clean, encode, and derive temporal/behavioral features; enqueue for real-time inference.

9. 2.AI Detection: Cost-sensitive ensemble (e.g., RF + XGBoost + LR meta) outputs a risk score [0,1][0,1][0,1] and fraud flag. Thresholds are tuned for high recall at low FPR.
10. 3.Explainability (XAI): Per-transaction reason codes via SHAP/LIME; store concise feature-attribution summaries to support audit and analyst triage.
11. 4.Integrity & Audit (Blockchain): Bundle {tx-ID, timestamp, risk, reasons, metadata} → hash; batch into a Merkle root; commit root on a permissioned blockchain; keep full evidence off-chain. Smart contracts track dispute states (OPEN → REVIEW → RESOLVED).
12. 5.UI & Monitoring: Analyst dashboard with live alerts, searchable case view linked to on-chain proofs, performance tiles (recall, PR-AUC), and data-drift monitors.
13. 6.Performance Path: Inline inference targets ≤0.25 s (p95); blockchain anchoring runs asynchronously in micro-batches to preserve throughput and integrity.

VI RESULTS

The proposed framework is expected to deliver a robust, interpretable, and tamper-proof system for online fraud detection and payment integrity. The combination of AI-driven analytics and blockchain-backed evidence management ensures both predictive efficiency and operational trustworthiness.

1.High Detection Accuracy:

The cost-sensitive ensemble model is designed to achieve high recall under extreme class imbalance, maintaining a recall rate of over 75% at a false positive rate below 1%. This ensures that even rare fraudulent events are effectively captured.

2.Explainable Decision Layer:

Each transaction will be accompanied by clear reason codes and feature-contribution maps, enabling analysts, auditors, and regulators to interpret the model's decision-making process in a transparent and accountable manner.

3.Immutable Evidence Management:

The blockchain layer provides verifiable and tamper-proof storage for every fraud decision, making post-event validation and dispute resolution completely traceable and secure.

4.Real-Time System Performance:

With optimized pipelines and asynchronous blockchain anchoring, the system is expected to process 95% of transactions within 0.25 seconds, ensuring compatibility with real-world payment environments.

5.Regulatory and Operational Trust:

The architecture supports auditability, transparency, and explainability, aligning with global financial governance standards and enhancing customer confidence in digital payment ecosystems.

6.Scalability and Adaptability:

The modular design allows integration with different financial platforms, continuous retraining through data-drift monitoring, and scalability to accommodate growing transaction volumes.

VII.REFERENCES

[1] J. West and M. Bhattacharya, "Intelligent Financial Fraud Detection: A Comprehensive Review," Computers & Security, vol. 57, pp. 47–66, 2016.

[2] A. Whitrow, D. Hand, P. Juszczak, D. Weston, and N. Adams, "Transaction Aggregation as a Strategy for Credit Card Fraud Detection," Data Mining and Knowledge Discovery, vol. 18, no. 1, pp. 30–55, 2009.

[3] C. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy," IEEE Transactions on Neural Networks and Learning Systems, vol. 29, no. 8, pp. 3784–3797, 2018.

[4] R. Chalapathy and S. Chawla, "Deep Learning for Anomaly Detection: A Survey," arXiv preprint arXiv:1901.03407, 2019.

[5] S. Jurgovsky et al., "Sequence Classification for Credit-Card Fraud Detection," Expert Systems with Applications, vol. 100, pp. 234–245, 2018.

[6] S. Carcillo, A. Dal Pozzolo, O. Caelen, Y.-A. Le Borgne, and G. Bontempi, "Scarff: A Scalable Framework for Streaming Credit Card Fraud Detection with Spark," Information Fusion, vol. 41, pp. 182–194, 2018.

[7] D. Gunning and D. Aha, "DARPA's Explainable Artificial Intelligence (XAI) Program," AI Magazine, vol. 40, no. 2, pp. 44–58, 2019.

[8] S. Lundberg and S.-I. Lee, "A Unified Approach to Interpreting Model Predictions," Advances in Neural Information Processing Systems (NeurIPS), 2017.

[9] M. Ribeiro, S. Singh, and C. Guestrin, "Why Should I Trust You?: Explaining the Predictions of Any Classifier," Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016.

[10] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," Applied Innovation Review, vol. 2, pp. 6–19, 2016.

[11] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," White Paper, 2008.

[12] X. Xu, I. Weber, and M. Staples, Architecture for Blockchain Applications, Springer, 2019.

[13] R. Rejeb, J. G. Keogh, and H. Treiblmaier, "How Blockchain Technology Can Improve Supply Chain Performance: A Systematic Review," IEEE Access, vol. 8, pp. 60722–60745, 2020.

[14] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557–564, 2017.