International Journal of Computing and Artificial Intelligence

E-ISSN: 2707-658X
P-ISSN: 2707-6571
www.computersciencejournals.com/ijcai
IJCAI 2025; 6(2): 33-36
Received: 05-05-2025
Accepted: 11-06-2025

Himat Singh
Assistant Professor of Computer Science, GAD Khalsa College, Chohla Sahib, Tarn Taran, Punjab, India

Corresponding Author:
Saeed Shoja Shafti
Assistant Professor of Computer Science, GAD Khalsa College, Chohla Sahib, Tarn Taran, Punjab, India

Blockchain-enabled fraud detection technique for secure transactions

Himat Singh

DOI: https://doi.org/10.33545/27076571.2025.v6.i2a.175

Abstract
As financial transactions increasingly migrate to digital platforms, fraud detection has become a critical area of concern for governments, businesses, and consumers. Traditional fraud detection systems, while effective to some degree, are often limited by their centralized architecture, vulnerability to tampering, and delayed response capabilities. This paper proposes a blockchain-based fraud detection framework that integrates smart contracts, immutable ledger design, and external data sources via oracles to improve real-time detection and prevention of fraudulent transactions. The system leverages blockchain's transparency and automation to enhance the integrity of transaction processing while reducing reliance on centralized oversight. This work is intended as a conceptual and architectural contribution, offering a detailed model and identifying key challenges and directions for future research.

Keywords: Blockchain, fraud detection, smart contracts, financial security, oracles, transaction integrity, tamper resistance, real-time monitoring, compliance auditing

1. Introduction
Digital financial transactions have grown exponentially in recent years, offering convenience and efficiency. However, this growth has been accompanied by an alarming rise in fraudulent activities, including identity theft, phishing, payment fraud, and fake merchant schemes. Traditional fraud detection methods, which typically involve rule-based systems or centralized machine learning models, are not only reactive but also susceptible to manipulation and lack robust auditability.

Blockchain technology, characterized by its decentralized and immutable ledger, presents a promising alternative. Introduced by Nakamoto (2008) [4], blockchain's primary features—transparency, consensus, and programmable logic—allow for trustless verification and tamper-resistant transaction records. When combined with smart contracts and secure data feeds, blockchain can provide real-time enforcement of fraud detection policies without requiring central intermediaries.

This paper proposes a conceptual framework that harnesses blockchain's core capabilities to detect and mitigate fraud in financial transactions. The aim of this research paper is to contribute to the evolving discourse on decentralized security infrastructure by outlining a model that integrates distributed ledger technology, smart contracts, and external data sources to detect and manage fraudulent behavior.

2. Literature Review
2.1 Traditional Fraud Detection Techniques
Conventional fraud detection systems rely on centralized data processing, statistical modeling, and supervised learning techniques to identify suspicious behavior. These systems are often siloed, reactive, and vulnerable to data manipulation. According to Zhang and Wen (2017) [7], rule-based systems tend to struggle with zero-day fraud patterns and require frequent updates.

2.2 Blockchain for Security and Transparency
Blockchain's immutable ledger and distributed consensus offer significant advantages for data security. Nguyen *et al.* (2020) [3] noted that blockchain technology can enhance accountability in digital banking by ensuring transparent and irreversible transaction

histories. This reduces the opportunity for malicious actors to tamper with historical records.

2.3 Smart Contracts and Automated Enforcement
Smart contracts are programmable scripts that execute predefined logic on the blockchain when certain conditions are met. Swan (2015) [2] emphasized their potential to eliminate intermediaries and automate enforcement of compliance and business logic. In the context of fraud detection, smart contracts can autonomously apply risk thresholds and transactional limits.

2.4 Data Oracles and External Intelligence
Since blockchains cannot natively access external data, oracles serve as trusted bridges to outside sources such as real-time fraud feeds, blacklists, and credit scoring platforms. Christodoulou *et al*. (2021) [1] acknowledged that oracles expand blockchain's applicability in dynamic and risk-sensitive environments.

2.5 Research Gap
While the benefits of blockchain for data integrity and transparency are well-documented, few studies integrate fraud analytics, smart contracts, and secure oracles into a unified, real-time detection framework. This paper aims to address this gap by proposing such architecture.

3. Proposed Architecture
The proposed blockchain-enabled fraud detection system is designed as a multi-layered architecture, combining on-chain integrity with off-chain intelligence. This hybrid design balances the transparency, trust, and immutability of blockchain with the flexibility and computational power of traditional analytics. Each component plays a specific role in securing the transaction lifecycle.

3.1 Immutable Blockchain Ledger
At the core of the system lies a permissioned blockchain network, such as Hyperledger Fabric, Quorum, or Corda. Unlike public blockchains (e.g., Ethereum), permissioned blockchains restrict participation to trusted entities such as banks, regulators, or payment processors. This approach offers enhanced control, scalability, and compliance alignment.
Every transaction in the system is:
- **Cryptographically signed** using digital signatures from the sender.
- **Timestamped** with precise event timing.
- **Recorded immutably** across all nodes in the network.

This ensures that once a transaction is validated and added to the blockchain, it cannot be altered or deleted. This feature forms the foundation of a tamper-evident audit trail, which is essential for forensic investigations, regulatory compliance, and legal evidence in cases of fraud.
Additionally, consensus mechanisms like Raft, PBFT (Practical Byzantine Fault Tolerance), or Kafka ordering in permissioned networks ensure that no single party can unilaterally alter the ledger. As a result, trust is distributed, and manipulation by insiders or malicious actors is minimized.

3.2 Smart Contracts for Real-Time Detection
Smart contracts are programmable scripts stored on the blockchain that execute automatically when predefined conditions are met. In the context of fraud detection, smart contracts serve as autonomous enforcement agents that continuously monitor and validate transaction behavior against preset rules.

Examples of rules encoded into smart contracts include
- **Transaction amount thresholds**: Blocking transactions exceeding a certain limit unless further authentication is provided.
- **Frequency analysis**: Flagging rapid transaction bursts from a single account or device that deviate from typical behavior.
- **Geo-IP inconsistencies**: Identifying and flagging logins or transactions from improbable or previously unseen locations.
- **Unusual customer/merchant behavior**: Detecting transactions outside of historical behavioral norms.

Once triggered, the smart contract can take automated actions, such as:
- **Rejecting** a suspicious transaction before it reaches settlement.
- **Freezing** an account to prevent further activity until manual review.
- **Logging** the event immutably on-chain for downstream auditing and legal processing.

The deterministic execution of smart contracts ensures that no external intervention can manipulate fraud detection policies once deployed, enabling predictable, transparent, and bias-free enforcement.

3.3 Trusted Oracles for Contextual Input
Blockchains operate in closed environments and cannot access external data directly. To enable real-time fraud detection, the system incorporates oracles—trusted middleware services that fetch and verify external data sources.
These oracles are responsible for delivering:
- **Customer behavior scores** (from third-party credit or risk-scoring platforms).
- **Fraud blacklists** (shared databases of known malicious accounts or IPs).
- **Regulatory watchlists** (e.g., FATF, OFAC, or AML compliance data).

Each oracle response is:
- **Cryptographically signed** to prove origin and authenticity.
- **Time-stamped** to ensure freshness and prevent replay attacks.
- **Delivered securely** to the blockchain using encrypted channels or multi-signature aggregation for higher integrity.

Incorporating oracles ensures that smart contracts have real-world awareness—allowing them to respond not only to static rule violations but also to evolving fraud trends, geopolitical risks, or behavioral intelligence from third-party vendors.

3.4 Optional Off-Chain Analytics Layer
To augment the rule-based logic of smart contracts, the

architecture optionally includes a machine learning (ML) engine running off-chain. This layer is designed to detect complex behavioral anomalies and adapt to evolving fraud patterns that rule-based systems may miss.

Key features of this off-chain analytics module:

- Uses supervised or unsupervised learning models (e.g., Random Forest, Isolation Forest, or LSTM networks).
- Analyzes historical transaction data, user-device interaction patterns, and contextual metadata.
- Generates real-time risk scores for incoming transactions.

These risk scores are then:

- Forwarded to the smart contract layer via a secure oracle, which allows on-chain logic to respond accordingly (e.g., enhanced due diligence or multi-factor verification).
- Logged on-chain if deemed high-risk, to provide an immutable record of risk assessment input.

This approach creates a hybrid fraud detection model, blending the transparency and enforcement power of blockchain with the learning capacity of AI, offering more adaptive and effective fraud mitigation.

3.5 Audit and Compliance Interface

An essential requirement in fraud management systems is the ability to trace decisions, justify actions, and provide verifiable evidence to regulatory bodies, internal auditors, or law enforcement agencies.

Because blockchain inherently maintains a chronological, tamper-proof log, it is ideally suited for post-incident audit purposes.

This audit interface provides:

- Immutable access logs showing when, why, and how a transaction was flagged or blocked.
- Event lineage tracking, detailing all interactions between smart contracts, oracles, and users.
- Compliance reports generated automatically based on on-chain data, suitable for financial reporting or court evidence.

By minimizing human intervention and manual logging, the system enhances transparency, accountability, and legal defensibility. Moreover, access controls can be applied to ensure role-based audit permissions—e.g., investigators may access only case-related records, while regulators may view system-wide trends.

4. Security and Operational Benefits

4.1 Tamper Resistance

The blockchain's append-only ledger ensures that once a transaction is confirmed, it cannot be altered or deleted. This prevents cover-ups or post-fraud manipulation.

4.2 Insider Threat Mitigation

Because rules are encoded into smart contracts and publicly verifiable (in public or consortium blockchains), internal fraud is harder to commit or hide.

4.3 Decentralized Trust

No single party can unilaterally validate a fraudulent transaction. Consensus mechanisms distribute authority, minimizing systemic risks.

4.4 Verifiable External Inputs

By using secure oracles, the system ensures that any decision based on external intelligence is both traceable and auditable.

5. Limitations and Challenges

While the proposed framework offers strong advantages, it also introduces several trade-offs:

- **Scalability**: Public blockchains may not support high-throughput fraud detection unless layer-2 solutions are implemented.
- **Privacy Concerns**: Sensitive data recorded on-chain could conflict with GDPR or data protection laws, unless zero-knowledge techniques are used.
- **Integration Barriers**: Legacy systems may resist integration due to architectural and regulatory constraints.
- **Smart Contract Vulnerabilities**: Poorly written contracts may be exploited unless rigorously audited.

6. Future Work

Future research should explore:

- Implementation of privacy-preserving fraud detection using zk-SNARKs or confidential transactions
- Federated fraud detection models that share anonymized fraud signals across institutions using blockchain
- Simulated environments to evaluate throughput, detection accuracy, and cost implications
- Alignment with global financial regulations, including KYC/AML compliance

7. Conclusion

This paper proposes a blockchain-based fraud detection model that integrates smart contracts, secure data feeds, and immutable audit trails. Unlike traditional systems, the proposed approach offers decentralized validation, real-time enforcement, and tamper-proof evidence. Although there are challenges around scalability, privacy, and interoperability, the architecture provides a forward-looking direction for securing financial transactions in the digital age. As blockchain matures and legal frameworks evolve, such models may become central to fraud prevention infrastructures.

8. References

1. Christodoulou K, Andreou A, Papadopoulos G. Blockchain for fraud detection: A systematic literature review. Computers and Security. 2021;108:102376. https://doi.org/10.1016/j.cose.2021.102376
2. Swan M. Blockchain: Blueprint for a New Economy. Sebastopol: O'Reilly Media; 2015.
3. Nguyen CT, Pathirana PN, Nguyen DC, Seneviratne A, Li W. Blockchain for secure e-commerce and digital banking. Journal of Systems Architecture. 2020;112:101804. https://doi.org/10.1016/j.sysarc.2020.101804
4. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available from: https://bitcoin.org/bitcoin.pdf

5. Alzahrani N, Bulusu N. Block-SIEM: Blockchain-based security information and event management. In: Proceedings of the IEEE International Conference on Communications (ICC); 2018. p. 1-6. https://doi.org/10.1109/ICC.2018.8422174
6. Kshetri N. Can blockchain strengthen the Internet of Things (IoT)? IT Professional. 2017;19(4):68-72. https://doi.org/10.1109/MITP.2017.3051330
7. Zhang Y, Wen J. An IoT electric business model based on the protocol of bitcoin. In: 2015 18th International Conference on Intelligence in Next Generation Networks (ICIN); 2015. p. 184-91. https://doi.org/10.1109/ICIN.2015.7073810
8. Atzori M. Blockchain technology and decentralized governance: Is the state still necessary? Journal of Governance and Regulation. 2017;6(1):45-62. https://doi.org/10.22495/jgr_v6_i1_p5
9. Wood G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper. 2014;1(1):1-32. Available from: https://ethereum.github.io/yellowpaper/paper.pdf
10. Mukkamala S, Janardhan N, Litchfield A, Nepal S, Xiang Y, Thabtah F. Credit card fraud detection using deep learning and blockchain integration. In: 2020 IEEE International Conference on Big Data (Big Data); 2020. p. 4477-86. https://doi.org/10.1109/BigData50022.2020.9378044