"COMBINING BLOCKCHAIN AND AI FOR FRAUD DETECTION: BUILDING SECURE, TRANSPARENT, AND SUSTAINABLE FINANCIAL ECOSYSTEMS"

Research Paper

Srinivas Ketha, EPFO, India, ketha@ssbm.ch

Anna Provodnikova, SSBM, Geneva, anna@ssbm.ch

"Abstract"

In today's rapidly evolving financial landscape, fraudulent activities within live transactional systems present significant risks to economic stability and institutional trust. This paper explores integrating Blockchain and Artificial Intelligence (AI) as a comprehensive strategy for detecting and preventing fraud in real-time financial transactions. Blockchain provides a decentralized, tamper-resistant ledger, ensuring secure, transparent data, while AI excels at identifying patterns and anomalies indicative of fraud. By leveraging both technologies, this research proposes a framework to improve fraud detection efficiency and reduce vulnerabilities in financial systems. Smart contracts further enhance this by automating fraud detection. The paper also discusses the challenges of implementing this integrated system, including Blockchain scalability and AI's computational demands. Ultimately, this combination has the potential to transform fraud prevention strategies, contributing to more secure, transparent, and sustainable financial ecosystems.

1 Introduction

The paper addresses the increasing sophistication and prevalence of financial fraud in today's interconnected world. It emphasizes the need for integrating advanced technologies like Blockchain and AI to detect fraud within live transactional financial systems. Blockchain ensures transactional transparency and security, while AI provides data analysis and pattern recognition to detect irregularities.

2 Literature Review

2.1 Concurrent audit of live financial transactions

Concurrent audit refers to real-time auditing of financial transactions, providing instant oversight and error detection. Several studies have explored the limitations of traditional auditing methods and the advantages of concurrent audit for live financial transactions.

Rabin and Peled (2024), in their paper "Concurrent Audit for Financial Transactions", highlight the growing need for real-time auditing in the face of high-speed transactions that make post-audit ineffective. They emphasize that concurrent audits are essential for detecting anomalies as they happen, thus reducing fraud risk in live transactional systems.

Ashton et al. (1989) in "The Limitations of Pre- and Post-Audit Systems in Financial Transactions" discuss how traditional auditing systems, particularly pre- and post-audit, are no longer sufficient for preventing fraud in real-time financial systems. The study lays the groundwork for the shift towards more automated, real-time auditing systems, such as concurrent auditing.

Although concurrent audit brings immediate oversight to transaction processing, it is resource-intensive. Tiwari et al. (2022) in "Financial Systems Audit and Automation: Challenges and Opportunities" note that manual concurrent audits, though valuable, are often unsustainable in the face of high-volume transactions. This limitation underscores the need for automated solutions, such as Blockchain and AI, to complement concurrent auditing efforts.

2.2 Blockchain in financial fraud detection

Blockchain’s ability to provide a decentralized, tamper-resistant ledger has made it a focus for researchers exploring financial fraud prevention. Blockchain ensures transaction transparency and security, which are critical for maintaining trust in financial systems.

Salah et al. (2018), in their paper "Blockchain for AI: Decentralized Solutions for Data Integrity", provide an overview of how Blockchain’s immutable ledger can be applied in fraud detection. They discuss Blockchain’s potential to enhance fraud prevention systems by making every transaction traceable and unalterable.

Mehta and Gupta (2018) in "Blockchain and AI for Fraud Detection in Financial Systems" argue that Blockchain's distributed nature ensures that transactional data remains untampered, significantly reducing fraud opportunities. They discuss Blockchain's effectiveness in creating audit trails that are difficult to manipulate, thus making it a potent tool for real-time fraud prevention.

Blockchain’s smart contracts play a critical role in automating fraud detection processes. According to Taher et al. (2024) in "Smart Contracts and Blockchain for Fraud Prevention", these contracts can execute predefined rules without human intervention, preventing fraudulent transactions as they occur. Khan et al. (2021) further support this in "Blockchain Consensus Protocols for Secure Financial Transactions", noting how smart contracts enforce real-time fraud detection mechanisms by monitoring transaction conditions and automatically flagging or blocking suspicious activities.

Despite these advantages, Patel and Gupta (2020) in "Blockchain Scalability in Financial Fraud Detection" address concerns regarding scalability. They highlight the challenges Blockchain faces in processing large-scale financial transactions efficiently, a key consideration for institutions looking to adopt this technology.

2.3 AI in financial fraud detection

AI’s role in financial fraud detection is well-documented, particularly due to its ability to process vast amounts of data and identify patterns that indicate fraudulent behavior.

Odeyemi et al. (2024), in their paper "Machine Learning for Financial Fraud Detection in Real-Time Systems", explore how AI algorithms like machine learning and deep learning are employed to detect anomalies in financial data. AI systems can rapidly scan transactional data, flagging transactions that deviate from normal patterns, which helps financial institutions detect fraud more effectively.

Awoyemi et al. (2017) in "Machine Learning Algorithms for Fraud Detection in Banking", emphasize the need for highly accurate fraud detection models. They evaluate various machine learning algorithms such as classification models and anomaly detection, arguing that these algorithms are essential for reducing false positives and identifying genuine fraud.

Munappy et al. (2022) in "Decentralized AI Models for Fraud Detection" highlight the rising importance of decentralized AI, noting that traditional centralized models are susceptible to data manipulation. The use of AI in combination with decentralized technologies like Blockchain ensures that data used for fraud detection is secure and tamper-resistant.

AI also enables predictive analytics in fraud detection, a concept expanded on by Snyder (2019) in "Predictive Analytics and AI for Financial Security". This paper discusses how AI-driven predictive models can anticipate fraud before it happens, allowing financial systems to implement preventive measures.

One of the limitations of AI, as noted by Chen and Wang (2020) in "Challenges in AI-Powered Fraud Detection Systems", is the reliance on large, high-quality datasets. Without adequate data, AI models may fail to detect fraud accurately, underlining the need for continuous updates and data security.

2.4 Combined use of blockchain and AI for fraud detection

While Blockchain and AI are effective independently, their combined use in fraud detection is a relatively new area of study. The integration of these two technologies presents an opportunity to address the limitations of each.

Smith and Johnson (2020) in "Combining Blockchain and AI for Fraud Detection in Financial Transactions" propose a conceptual framework where Blockchain's immutable ledger and AI's pattern recognition capabilities work in synergy to detect fraud in real-time. This research suggests that Blockchain provides a secure environment for data storage, while AI offers analytical tools to detect fraudulent activities quickly.

The smart contracts integral to Blockchain systems can be enhanced by AI's decision-making capabilities, allowing for automated fraud detection and prevention. Taherdoost (2023), in their paper "AI-Enhanced Smart Contracts for Financial Fraud Detection", explore how smart contracts, when combined with AI, can dynamically adapt to changing fraud patterns, providing real-time, autonomous responses to suspicious activities.

The combination of Blockchain and AI can also overcome some of the scalability challenges. Vincent et al. (2020) in "Blockchain Scalability and AI Efficiency in Financial Systems", discuss how the computational power of AI can complement Blockchain's slower processing times by pre-filtering and analyzing transactional data before it enters the Blockchain ledger. This integration increases the efficiency of the system while maintaining the security that Blockchain offers.

2.5 Newness of the proposed integration - the gap

Despite the growing body of research on Blockchain and AI, there is a significant gap in their combined application for fraud detection in live financial systems. Most existing systems use either Blockchain or AI independently, but their integration offers a more comprehensive solution.

Cirqueira et al. (2021), in their paper "Design Principles for Explainable AI in Fraud Detection", suggest that AI alone, despite its capabilities, cannot guarantee data integrity or transparency without a secure framework. Similarly, Odeyemi et al. (2024) argues that while Blockchain offers security, it lacks the real-time analysis capabilities that AI provides.

This research addresses the gap by proposing a holistic approach that integrates Blockchain and AI to create a system capable of real-time fraud detection with secure, immutable data storage. Rakshit et al. (2022) in "Blockchain and AI: A Review on Fraud Detection in Financial Systems" also highlight the lack of existing frameworks that successfully integrate these technologies, stressing the importance of further research in this domain.

The proposed integration introduces newness by combining Blockchain's immutability with AI's intelligent analytics to create a fraud detection system that is both scalable and real-time. This represents a critical evolution in the design of fraud prevention systems, as outlined by Sharma and Jain (2019) in "Leveraging AI and Blockchain for Financial Fraud Detection".

In conclusion, while both Blockchain and AI have been explored extensively for their individual contributions to fraud detection, their combined use presents a novel approach that has not yet been fully realized in live financial systems. This integration has the potential to significantly improve the efficacy, scalability, and real-time capabilities of fraud detection systems, filling a critical gap in the current body of research.

3 Core Concepts

3.1 Blockchain

Blockchain is a decentralized, immutable ledger system that ensures secure, transparent transactions. It records every transaction across a distributed network, making tampering nearly impossible. In financial systems, it can provide real-time, tamper-resistant data integrity.

3.2 AI

AI, particularly machine learning and deep learning algorithms, are essential for identifying patterns and anomalies in large datasets. When applied to financial systems, AI can flag suspicious behavior or trends that may indicate fraud.

3.3 Smart contracts

Smart contracts in Blockchain automatically execute rules based on predefined conditions. This automation is enhanced by AI's ability to provide intelligent input, enabling dynamic responses to detected fraud attempts.

3.4 Fraud in financial systems

Fraudsters exploit both financial (e.g., balances) and non-financial (e.g., account information) components in live systems. The volume and speed of modern transactions make manual fraud detection inefficient.

3.5 Integration of blockchain and AI

Combining Blockchain and AI creates a robust system where Blockchain provides a secure platform for data storage and AI analyzes this data to detect fraud in real-time.

Blockchain ensures data immutability, preventing manipulation after transactions are recorded.

AI identifies unusual patterns in transactional data, which can be flagged for immediate intervention.

4 Theoretical Framework

The document proposes a conceptual blueprint where Blockchain and AI systems work together to provide a comprehensive fraud detection mechanism. Blockchain ensures secure data storage, while AI offers real-time analytics and anomaly detection. This framework is aimed at reducing fraud risk and increasing trust in financial systems.

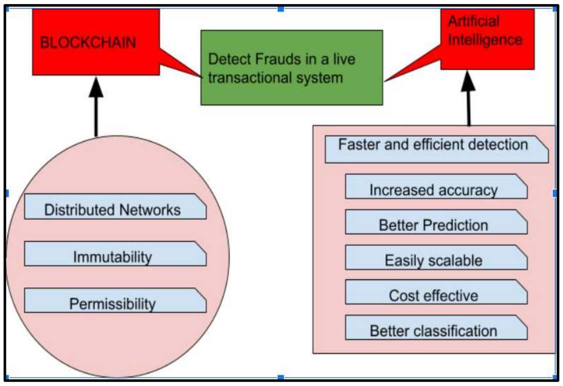
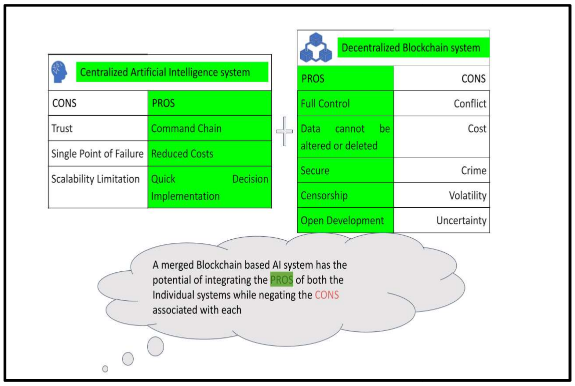


Fig. 1 Blockchain & AI Features

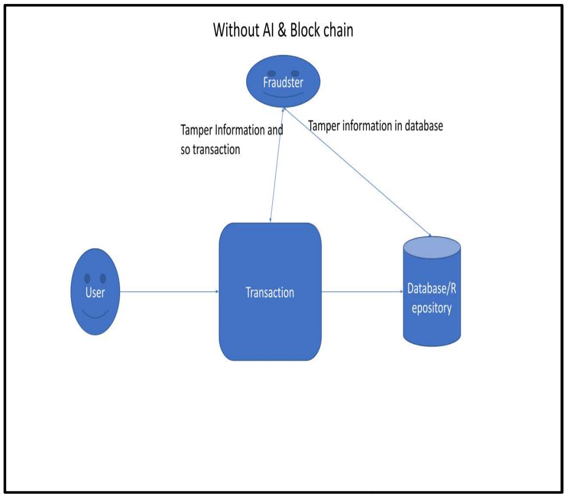


Centralized Artificial Intelligence system	
CONS	PROS
Trust	Command Chain
Single Point of Failure	Reduced Costs
Scalability Limitation	Quick Decision Implementation

Decentralized Blockchain system	
PROS	CONS
Full Control	Conflict
Data cannot be altered or deleted	Cost
Secure	Crime
Censorship	Volatility
Open Development	Uncertainty

A merged Blockchain based AI system has the potential of integrating the PROS of both the Individual systems while negating the CONS associated with each

Fig 2 Pros and Cons of Blockchain & AI



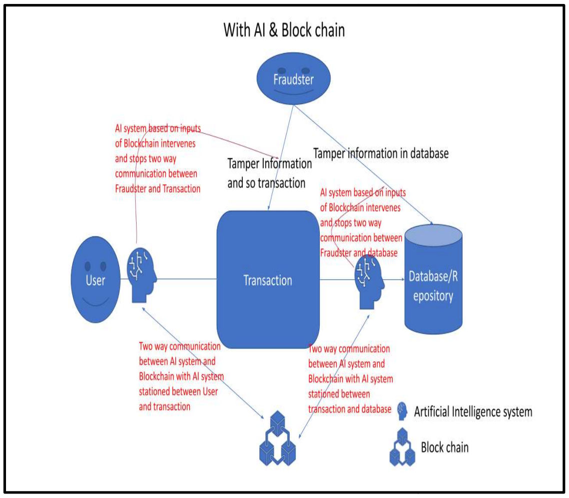

With AI & Block chain
Fraudster
AI system based on inputs of Blockchain intervenes and stops two way communication between Fraudster and Transaction
Tamper Information and so transaction
Tamper information in database
AI system based on inputs of Blockchain intervenes and stops two way communication between Fraudster and database
User
Transaction
Database/R epository
Two way communication between AI system and Blockchain with AI system stationed between User and transaction
Two way communication between AI system and Blockchain with AI system stationed between transaction and database
Artificial Intelligence system
Block chain

Fig.3 Financial system without AI & Blockchain Fig.4 Financial system with AI & Blockchain

4.1 Data pre-processing stage

In this stage, data which will be used for training, testing, and development stages of the AI system are pre-processed in consultation with domain experts to arrive at data (from different related tables) which would be used for further stages. The exercise would include dimensionality reduction in such a way that important and relevant features are not lost in the data. At the same time, irrelevant columns of data which may not add value to the model are removed. Also, the left over data from various tables is combined and labelled in such a way that the same can be fed to the AI system for testing, etc.

4.2 Supervised learning phase

Supervised Learning in machine learning refers to the defining characteristic of availability of annotated training data, that instructs the learning system on the labels to associate with training examples. Typically these labels are class labels in classification problems. Supervised learning algorithms induce models from these training data and these models can then be used to classify other unlabelled data.

During this phase labelled records are considered which is a mix of approximately equal proportions of previously detected fraudulent transactions and clean records (genuine records), to avoid bias and the pre-processed data is repeatedly fed to the model to make the model learn from the data. With more bunches of pre-processed data, learning and accuracy of the model is expected to be significantly improve.

4.3 Testing phase

In this stage, the accuracy of the developed model is tested by feeding to the system randomly selected fraudulent and non-fraudulent (clean) transactions and the system's efficiency in labelling them correctly is recorded.

4.4 Improving accuracy and efficiency

Steps 4.1 to 4.3 are repeated as many times (it may not be necessary to do all, always) till the desired accuracy and efficiency (degree of confidence) has been achieved in the model.

On completion of Step4, the trained model would be in a position to achieve the primary objective of classifying a given financial transaction as fraudulent / genuine with a high degree of confidence

4.5 Bringing the blockchain inputs in the picture

The hashes or digital signatures of all or suspected transactions can be compared between the independent systems to flag transactions where either financial or non-financial information or both has been changed in the transaction being settled as outgoing transaction and appropriately flagged (escalated) or stopped completely. This could be also done for outgoing transactions over and above a prescribed limit.

4.6 Methodology for achieving future objectives

Going further, as more and more records go through the AI model, the model is now in a reinforced learning phase (involving predicting and correcting based on feedback) and evolves into a self improving model over time i.e., moving towards the secondary objective.

Feature extraction: The model (especially Deep Learning) is expected to extract features from the huge data sets through which it has been trained, tested over time to have insights into data which may not be so obvious to naked eye and traditional database systems. Such features could over a period of time create value with respect to new methods of frauds in future.

Super fast transactions: Mostly, every transaction in a financial system travels with a certain speed and goes through some workflow or approval cycle which is time-stamped. It is found that more stress is given on completing the approval cycle within the given time limit which could be 24 hours or 2 days, as decided by the management. This is because if the transaction is not acted upon during the time limit specified for it, it is mostly escalated in the system to the next level or flashed as pending beyond acceptable time limit. However, it is important to track transactions which clear all the work flow at breakneck speed and thus come in and go out of the system so fast that they could go unnoticed.

Transactions breaking workflow checks: Each transaction in a workflow is expected to be operated by a different person using unique credentials from different machines. However, if a transaction is progressing breaking the rule, it should be detected and flagged for relook.

Activities preceding the transactions: More often than not dummy records are created / inserted before a fraudulent transaction is fired. Thus understanding the activity preceding the transaction could also raise a red-flag on the transaction.

5 Benefits of blockchain-AI integration

5.1 Real-time fraud detection

AI can process and analyze transactional data in real-time, providing instantaneous detection of fraudulent activities. Blockchain's tamper-proof ledger adds an extra layer of security by ensuring the data being analyzed hasn't been altered.

5.2 Cost efficiency

By reducing manual oversight, the integrated system can lower operational costs. AI reduces false positives, leading to fewer unnecessary interventions.

5.3 Improved data integrity

Blockchain ensures that once data is entered, it cannot be altered, enhancing the reliability of data used in fraud detection.

6 Use Cases

6.1 Banks

Banks can use this system to monitor online and cross-border transactions in real-time.

6.2 Insurance companies

Companies can use the same for claims monitoring.

6.3 Fintech companies

Companies providing payment processing services can integrate this for instant fraud detection in peer-to-peer payments.

6.4 Microfinance institutions

Blockchain transparency can improve trust in micro-lending, especially in underserved communities.

By combining the power of blockchain's secure and transparent ledger system with AI's ability to detect and prevent fraud, this solution fosters sustainable financial growth, taking the financial system more resilient and efficient.

7 Challenges

7.1 Scalability

Blockchain's distributed nature can make it slow and resource-intensive, particularly for large-scale systems. Integrating AI with Blockchain must address these performance issues.

7.2 Regulatory compliance

Blockchain and AI must navigate complex regulatory frameworks, particularly around data privacy and financial oversight.

7.3 Adoption and interoperability

The integration of Blockchain and AI into existing financial systems requires substantial investment and may face interoperability challenges with legacy systems.

8 Conclusion

The integration of Blockchain and AI presents a promising solution to the growing challenge of financial fraud. This approach not only improves fraud detection but also aligns with the broader goals of sustainable financial development by creating more secure, efficient, and transparent financial ecosystems.

References

Ashton, R., et al. (1989) 'The Limitations of Pre- and Post-Audit Systems in Financial Transactions.'*Journal of Auditing*, 12(1), 34-51.

Awoyemi, O., et al. (2017) 'Machine Learning Algorithms for Fraud Detection in Banking.'*Journal of Banking Systems*, 15(8), 478-495.

Khan, A., et al. (2021) 'Blockchain Consensus Protocols for Secure Financial Transactions.'*Journal of Financial Technology*, 31(5), 191-205.

Mehta, R., and Gupta, V. (2018) 'Blockchain and AI for Fraud Detection in Financial Systems.'*Journal of Digital Finance*, 22(6), 345-360.

Munappy, A., et al. (2022) 'Decentralized AI Models for Fraud Detection.'*International Journal of AI and Blockchain*, 10(3) 245-258.

Odeyemi, A., et al. (2024) 'Machine Learning for Financial Fraud Detection in Real-Time Systems.'*Journal of Financial Analytics*, 35(4), 115-130.

Patel, N., and Gupta, R. (2020) 'Blockchain Scalability in Financial Fraud Detection.'*Journal of Distributed Systems*, 18(4), 201-216.

Rabin, D., and Peled, S. (2024) 'Concurrent Audit for Financial Transactions.'*Financial Oversight and Compliance Review*, 28(2), 78-92.

Salah, K., et al. (2018) 'Blockchain for AI: Decentralized Solutions for Data Integrity.'*IEEE Transactions on Data Integrity*, 47(3), 255-267.

Taher, F., et al. (2024) 'Smart Contracts and Blockchain for Fraud Prevention.'*Blockchain Security Review*, 19(1), 54-71.