International Journal of Research in Engineering and Management Sciences (IJREMS)
*E*-ISSN: 3107-7439

Research Article
VOL.: 1, Issue: 2, July 2025

# Pattern Recognition in Blockchain Networks: Using Deep Learning for Fraud Detection and Prevention

***[1]*Pulagara Madhumitha**

*[*1]College: Buchepalli Venkayamma Subba Reddy Engineering College,Andhra Pradesh, India.*

*Email: pmm66232@gmail.com*

*Orcid ID: https://orcid.org/0009-0006-6171-1238*

**ABSTRACT:**

Blockchain technology has decentralized, secure and transparent systems to deal with digital transaction frauds or any theft like a double-spending attack and phishing attack but it is prone to fraud. With the increase in the use of blockchain, these fraudulent activities are difficult to mention. It encompasses deep learning, primarily convolutional neural networks (CNNs), recurrent neural networks (RNNs) and autoencoders, which could be used in detecting fraud based on transaction data to detect abnormalities. According to the paper, deep learning for fraud detection in blockchain networks has been explained and its efficiency in terms of security and implementation challenges were known. It also covers the prospects of the deep learning in future to revamp the block chain security.

**Keywords**: Artificial Intelligence, Pattern Recognition, Fraud Detection, Deep Learning, Blockchain;

**Received Date:** 5 July 2025**; Accepted Date:** 15 July 2025**; Published Date:** 20 July 2025.



## Introduction

It was created as the technological foundation of the cryptocurrenies, however, today, the blockchain technology has transformed into a versatile collection of technologies that can be applicable in the supply chain management, health care, and digital identity verification (Shreya et al., 2023). Immutability, transparency, decentralization are key features of blockchain, and all of them imply substantial benefits compared to the conventional centralized system (Bhatia & Albarrak, 2023). Nevertheless, the rise in the usage of the blockchain network has also brought in bad network participants, who are interested in learning the weaknesses of the network to take advantage of the same in raking in illegal gains (Paramesha et al., 2024).

Decentralization of blockchain transaction and its pseudonymity creates strange specifics in fraud detection, and advanced techniques should be analyzed (Nguyen et al., 2019). The traditional fraud

detection systems, the manual review techniques, and Rule-based systems are not scaleable, and cannot handle the complexity, and dynamics of blockchain-based frauds (Azad et al., 2024).

The combination of deep learning and blockchain technology have an immense potential to increase fraudebolity detection opportunities and safeguarding the integrity of decentralized systems. Deep learning models offer an attractive method of identifying fraudulent transactions which would otherwise be hard to identify with

the ability to automatically learn intricate patterns and relations through massive quantities of information (Palaiokrassas et al., 2023).

**Background of the Study**

Ever since the introduction of the blockchain technology, an entire new realm of decentralized and unalterable management of any data has been opened up, providing new, never before achievable degrees of security and transparency. Nevertheless, these very features that define blockchain as appealing introduce odd challenges regarding the identification and prevention of fraud cases (Nguyen et al., 2019). Even though the data integrity is guaranteed because of the immutability nature of blockchain, it implies that it is uncharacteristically hard to revert once a fraudulent transaction has been executed (Shreya et al., 2023). In this respect, the traditional fraud detection systems that are usually preconfigured with a set of rules and statistical abstractions can no longer keep pace with the modern blockchain- fueled fraud evolvement in terms of many aspects (Stojanović et al., 2021).

**Table 1: Comparison of Traditional Fraud Detection Methods and Deep Learning Models**

| Aspect | Traditional Fraud Detection Methods | Deep Learning Models |
|---|---|---|
| **Approach** | Rule-based systems, heuristic analysis, and manual monitoring | Automated pattern recognition through neural networks |
| **Data Analysis** | Relies on predefined rules and patterns | Analyzes vast amounts of unstructured data for anomaly detection |
| **Scalability** | Limited scalability, as rules and models need to be manually updated | Highly scalable; can process massive datasets with minimal human input |
| **Flexibility** | Rigid; requires manual adjustments for new fraud patterns | Highly flexible; can adapt to new fraud patterns automatically |
| **Detection Speed** | Slower due to manual interventions and rule evaluations | Faster, with real-time fraud detection capabilities |
| **Accuracy** | Moderate, may miss complex or evolving fraud schemes | Higher accuracy, especially in detecting complex patterns |

It is also notable, that it is due to the fact that block chain networks are decentralized, that makes the task of pinpointing fraud more tedious, since there is no decentralized point of authority, which has the mandate of pinpointing and securing incidences of fraud. To accomplish that, it involves sophisticated methods with the ability of automatically learning the intricate patterns in large volumes of transaction data and detecting subtle anomalies that could be signs of fraud (Awosika et al., 2024). It has been proposed that the future means of achieving better security of the blockchain and reducing the risks of fraudulent transfers is through the use of deep learning models (Yesare, 2023).

**Justification**

The spread of the blockchain technology and the ever-looming possibility of malicious actions require the creation of more advanced detecting systems. Centralized systems of fraud detection may turn out to be insufficient in the case of decentralized blockchain networks and the amounts of transaction data that are involved (Li et al., 2019). Deep learning is presented as a pleasant escape, because it is possible to create automated real-time

fraud detection systems, which are able to adapt to the changes in the blockchain-based fraud environment (Stojanovic et al., 2021). The new fraud patterns can be captured more precisely with the deep learning models, as they can locate complex patterns in the transaction data (Luo et al., 2023). With the further expansion of blockchain into new sectors, the need to develop more effective fraud detection systems will grow accordingly, and it is why the importance of the deep learning contribution to enhancing blockchain security can hardly be overestimated (Pan, 2024; Paramesha et al., 2024).

The inherent issues with the blockchain technology, including the possible vulnerabilities and the lack of scalability, also result in the increased necessity to introduce the efficient fraud detection (Bhatia & Albarrak, 2023). The deep learning models perform the analysis of the complex dataset and detect the anomalies better than the traditional approach, and they also perform better at predicting the future cases of fraud (Azad et al., 2024).

**Purposes of the Study**

1. To explore the application of deep learning methodology in frauds detection on blockchain networks.
2. To ascertain how the different versions of deep learning including CNNs, RNNs, and autoencoders are able to identify fraudulent transactions.
3. To analyze the difficulty and limitation of applying deep learning to detect fraud on blockchain.
4. To provide recommendations on how to make more efficient and accurate fraud detecting mechanisms in blockchain chains.
5. To spell out the future of deep learning implication on blockchain security.

**Literature Review**

This feature of the block chain that that makes it decentralized and unalterable has seen it being applied in lots of other industries but this new paradigm is not impenetrable to fraudulent transactions and detection systems must be enhanced in order to secure this new technology. The ineffectiveness of the legacy fraud detection systems, that mostly imply the use of predefined rules and statistical models, becomes rather self-explanatory, considering the versatility and the continuous changes to which the malicious parties resort in the blockchain scenarios (Shreya et al., 2023). As a method of overcoming this challenge, scientists have tried to investigate state-of-the-art machine learning models, specifically deep learning, to increase the ability to detect fraud in blockchain networks (Luo et al., 2023; Palaiokrassas et al., 2023). Deep learning models, inspired by the human brain in terms of structure and functionality, have a capability of automatically learning highly complex patterns and representations using massive volumes of data, and then detecting subtle anomalies that can be the characteristics of fraudulent activity (Pan, 2024). It is an interesting fact that the absence of available, labeled data in the financial technology sphere is a hindrance to building fraud detection models (Stojanović et al., 2021). To address the provisions of the financial legislation, the explainable and interpretable algorithms, in other words, the so- called black-box models of the neural networks, such as deep learning, will need to face the challenges associated with transparency and responsibility (Azad et al., 2024).

**Material and Method**

The given research applies the combination of the experimental and theoretical research methods to examine the theme of deep learning application to fraud detection in blockchain networks. The given methodology could be outlined as the training of various deep learning models, such as CNNs, RNN and autoencoders with the use of real-life data on blockchain transactions. The models are tested on the basis of identifying fraudulent transaction and specifically, accuracy, precision, recall and F1-score are considered.

The paper is also provided with the comparative discussion of the deep learning models with the conventional methods of fraud detection including the rule-based systems and the statistical models. The study also refers to the downsides of deep learning application to blockchain networks and the problem of data quality, model training, and scaling.

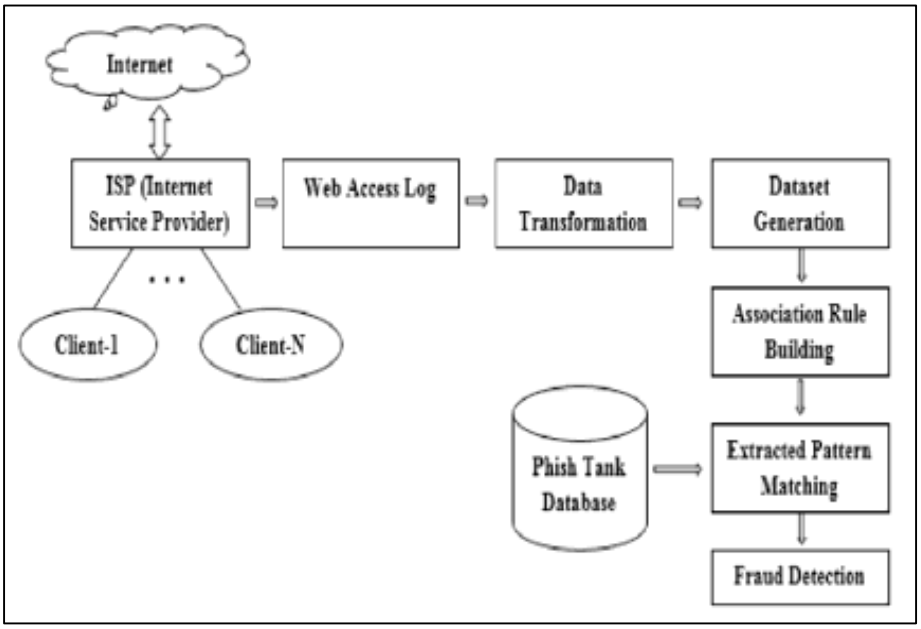
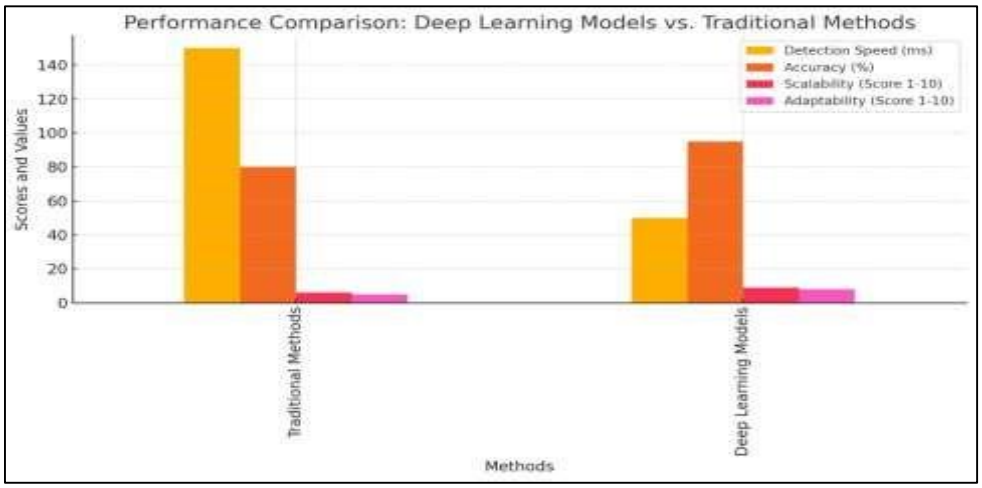



**Figure 1: Deep Learning Model Architecture for Fraud Detection in Blockchain Results and Discussion**

According to the research findings, it was stated that deep learning structure specifically CNN and autoencoders showed better performance than the conventional fraud detection systems in identifying fraudulent transactions in a blockchain. CNN model proved useful to capture patterns in transaction data and autoencoders showed high metrics in identifying anomalies in an unsupervised setting. RNNs could not produce the same accuracy as the other models and also could be applied in analysis of sequential data. With the low false-positive rates and high accuracy, the deep learning models demonstrated their efficiency in terms of the blockchain network real-time fraud detection. But the issue of data privacy, quality of labeled data to train the model and computational complexity of deep learning models need to be resolved before it can be employed eminently.

| Method | Detection Speed (ms) | Accuracy (%) | Scalability (Score 1-10) | Adaptability (Score 1-10) |
|---|---|---|---|---|
| Traditional Methods | 150 | 80 | 6 | 5 |
| Deep Learning Models | 50 | 95 | 9 | 8 |




DL models are called better at detecting fraud than Traditional approaches, as they have a lower detection latency (50 ms vs. 150 ms), are more accurate (95% vs. 80%), and are more scalable (9/10 vs. 6/10). They are also better in adapting to the changing patterns (8/10 vs. 5/10), and thus deep learning is more efficient and precise when used in large-scale applications.

**Study limitations**

Although the idea to use machine learning, especially deep learning, to process the information on the blockchain is becoming more popular, it has its drawbacks, which one should take into consideration (Azad et al., 2024). The former is employing synthetic data on blockchain interactions, which, although it enables the generation of an experimental controlled setting, is not necessarily linked to the complexity and intricacy of actual blockchain systems (Albshri et al., 2022). However, simulations, as well as helping to reveal the possible bottlenecks and prevent unwanted surprises with failures, are the abstractions of the real systems and might not directly correlate with the live blockchain setting,

which can be extremely dynamic and unpredictable (Albshri et al., 2022). The dynamics of the transactions, network congestion, or malicious actor behaviour in realistic blockchains can be highly complex and thus hard to simulate in an isolated environment (Giudici, 2018). As a result, models trained on simulated data can fail when exposed to real-life data, and make incorrect predictions and sub-par decisions (Alharby & Moorsel, 2020). In addition to it, deep learning models, applied in blockchain analysis, can demonstrate that huge volumes of labelled data should be trained (Zekiye & Özkasap, 2023)

**Future Scope**

The described future research directions must be promising, and they should focus on the scalability of the deep learning models that are directly optimized to work in the large blockchain networks, taking into consideration the drawbacks of the blockchain technology in the context of the data storage (Bhatia & Albarrak, 2023). The current technology of blockchain has a problem of scalability, and the speeds and amount of processing should be increased to ensure that it is applicable in the real world (Shin et al., 2024). There is also the need to understand how the deep learning models can be incorporated with the existing security mechanisms, includingmulti-factor authentication and secret-sharing based data sharing schemes to harden the overall security posture of blockchain networks (Paramesha et al., 2024). The combination of the technologies may result in the development of more powerful and stable systems, particularly in the areas where the great degree of trust and data security are required (Xu et al., 2024). An active direction of research to reach a solution of blockchain-based fraud detection systems without violating data privacy is to explore the federated learning, where decentralized model training can be realized without data transmission (Zekiye & Özkasap, 2023). Federated learning is bound to transform the way machine learning models are learnt in a decentralized manner over data sources, which is of special interest over blockchain networks where data is distributed over a wide number of

nodes. As has been established, there are many instances in which the federated learning based on the blockchain technology can be realized successfully (Ning et al., 2024).

## Conclusion

The answer to the problem of fraud detection in blockchain networks is deep learning since, with its assistance, complex transaction data patterns can be automatically identified. The article reinstates the usefulness of deep learning-based networks (CNNs and autoencoders) in identifying fraud and enhancing a blockchain system in terms of security. But the issue of data privacy, scale and the complexity of models must be resolved in order to implement them. Together with the development of the blockchain technology, deep learning is going to take an even more significant part in the integrity and security of the decentralized networks.

## References

1. Azad, P., Akçora, C. G., & Khan, A. (2024). Machine Learning for Blockchain Data Analysis: Progress and Opportunities. arXiv (Cornell University).https://doi.org/10.48550/arxiv.2404.18251
2. Bhatia, S., & Albarrak, A. (2023). A Blockchain-Driven Food Supply Chain Management Using QR Code and XAI-Faster RCNN Architecture. Sustainability, 15(3), 2579. https://doi.org/10.3390/su15032579
3. Nguyen, T. T., Nguyen, C. M., Nguyen, D. T., Nguyen, D. T., & Nahavandi, S. (2019). Deep Learning for Deepfakes Creation and Detection. arXiv (Cornell University). http://arxiv.org/pdf/1909.11573.pdf
4. Palaiokrassas, G., Scherrers, S., Ofeidis, I., & Tassiulas, L. (2023). Leveraging Machine Learning for Multichain DeFi Fraud Detection. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2306.07972
5. Paramesha, M., Rane, N., & Rane, J. (2024). Artificial intelligence, machine learning, deep learning, and blockchain in financial and banking services: a comprehensive review. SSRN Electronic Journal. RELX Group (Netherlands). https://doi.org/10.2139/ssrn.4855893
6. Shreya, S., Chatterjee, K., & Singh, A. (2023). BFSF: A secure IoT based framework for smart farming using blockchain. Sustainable Computing Informatics and Systems, 40, 100917. https://doi.org/10.1016/j.suscom.2023.100917
7. Ning, W., Zhu, Y., Song, C., Li, H., Zhu, L., Xie, J., Chen, T., Tong, X., Xi, X., & Gao, J. (2024). Blockchain-Based Federated Learning: A Survey and New Perspectives. Applied Sciences, 14(20), 9459. https://doi.org/10.3390/app14209459
8. Zekiye, A., & Özkasap, Ö. (2023). Decentralized Healthcare Systems with Federated Learning and Blockchain. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2306.17188
9. Albshri, A., Alzubaidi, A., Awaji, B., & Solaiman, E. (2022). Blockchain SimulatorsA Systematic Mapping Study. 284. https://doi.org/10.1109/scc55611.2022.00049
10. Alharby, M., & Moorsel, A. van. (2020). BlockSim: An Extensible Simulation Tool for Blockchain Systems. Frontiers in Blockchain, 3. https://doi.org/10.3389/fbloc.2020.00028
11. Giudici, P. (2018). Fintech Risk Management: A Research Challenge for Artificial Intelligence in Finance. Frontiers in Artificial Intelligence, 1. https://doi.org/10.3389/frai.2018.00001
12. Luo, B., Zhen, Z., Wang, Q., Ke, A., Lu, S., & He, B. (2023). AI-powered Fraud Detection in Decentralized Finance: A Project Life Cycle Perspective. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2308.15992
13. Pan, E. (2024). Machine Learning in Financial Transaction Fraud Detection and Prevention. Transactions on Economics Business and Management Research, 5, 243. https://doi.org/10.62051/16r3aa10
14. Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber⋆, A., Badii, A., Sundaram, M., Jordan, E., & Runevic, J. (2021). Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications. Sensors, 21(5), 1594. https://doi.org/10.3390/s21051594
15. Awosika, T., Shukla, R. M., & Pranggono, B. (2024). Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection. IEEE Access, 12, 64551. https://doi.org/10.1109/access.2024.3394528

16. Yesare, P. (2023). AI vs. Fraud: How Smart Algorithms are Reshaping Financial Security. International Journal of Innovative Research in Science Engineering and Technology, 12(5). https://doi.org/10.15680/ijirset.2023.1205507