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

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

# Exploring AI-Driven Approaches to Enhance Blockchain Forensics in Cryptocurrency Fraud Detection

***[1]Dr. K. Vaishali***

*[*1]Professor, Jyothishmathi Institute of Technology and Science, Karimnagar, Telangana, India*
*Email: vaishali5599@dgmail.com*
*Orcid ID: https://orcid.org/0009-0006-6171-1238*

**ABSTRACT:**

In this paper, the author would elaborate on how Artificial Intelligence (AI) and machine learning (ML) may be utilized to improve blockchain forensics in detecting cryptocurrency frauds. Although blockchain provides a safe platform to carry out transactions using cryptocurrencies, fraudster transactions, including double-spending and money laundering, are major demerits. Scalability and efficiency are two downsides of the conventional approaches to blockchain forensics. According to the paper, AI-based (supervised and unsupervised) machine learning models may be applied to process blockchain information and better identify suspicious transactions. Their outcomes have revealed that the AI models including the decision trees, neural networks, and support vector machines are efficient in identifying complex fraud patterns compared to the traditional approaches. The paper has clarified that both AI and ML solutions will find their applicability in making the blockchain more secure and countering the intelligence of cryptocurrency frauds that is so far on the rising trend.

**Keywords**: Blockchain Forensics, Cryptocurrency Fraud, Artificial Intelligence, Machine Learning, Fraud Detection

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



## Introduction

AI and ML is the recent paradigm of blockchain forensics and is likely to transform the method of how malicious transactions are detected within the cryptocurrency ecosystem. Rule-based engine and manual observation based traditional solutions would not be able to keep pace with the number of transactions as well as complexity on blockchain and thus more elaborate and automation focused solutions are needed (Sowmya & Sathisha, 2023). That AI algorithms can process large amounts of information, find minor patterns that could be attributed to fraudulent activity, and detect deviant behavior that would not have been viewed in a regular manner of perceiving it is very useful. With the help of AI-enhanced blockchain forensics, one can exploit the already existing transparency of the blockchain technology, simultaneously decreasing the disadvantages of anonymity and pseudonymity which are largely misused by malicious actors (Adhikari et al., 2024). The application of AI to the

sphere will allow developing more professional forensic tools that would be capable of tracing and identifying malicious activity and securing blockchain networks on a long-term basis (Yesare, 2023). AI also leads to invention in the creation of new financial products and services and digitalization of the financial sphere and blockchain technology (Paramesha et al., 2024). It is becoming increasingly unavoidable to stack effective defensive AIs because the criminal tendencies are becoming exceedingly intricate, tailored, and elusive (Kurshan et al., 2024).

**Background of the Study**

Blockchain forensics is an emerging practice area which concerns the analysis and investigation of transactions on blockchain networks and applies data analysis and forensic investigation processes. The fact of transparency of the blockchain technology, in its turn, offers an unique opportunity to trace the trails of the illegal activity, including the instances of the double- spending, transaction laundering, and all the other branches of the cryptocurrency fraud (Yesare, 2023). The latter, in its turn, is compensated by the volume and the ever-increasing complexity of the blockchain data, which poses a formidable challenge to the conventional forensic process (Dasaklis et al., 2021). Due to the benefits of decentralization, ideally, blockchain networks are decentralized, and this implies that there is no central governing entity that monitors the transactions that occur within the network; this is an advantage in security and transparency, though it also implies that illegal activities performed on such networks are more difficult to trace (Dasaklis et al., 2021). However, the criminals have perfected the utilization of this decentralized design to launder money via complex services such as mixing services and obfuscation tools that conveniently come in to efficiently shake hands with the origin and the destination of the dirty money (Turner et al., 2020). Heuristic Traditional blockchain forensics has previously been conducted through the use of legitimate transactions which are manually marked as suspect and transaction patterns are examined to determine whether there may have been fraud involved. However, such methods are time-consuming in nature, resource-intensive, and quite often fail to uncover more sophisticated fraud schemes (Hossain, 2023). The use of AI and ML in blockchain forensics has been identified as an effective way of automatizing the fraudulent transaction detection mechanism, and it can be referred to as a genuine breakthrough in the war on crime when it comes to blockchain (Paramesha et al., 2024).

**Justification**

Such cross-sectoral contamination of the blockchain technology has also been accompanied by a proportional rise in financial malpractices that envelop the cryptocurrencies, hence the urgent requirement to devise effective solutions in the shape of blockchain forensic tools (Brotsis et al., 2019). The transactions in blockchain are digital, and it introduces peculiarities to the developed forensic practices and demands new methods to ensure the integrity and authenticity of the digital evidence that could be presented in the court (Lone & Mir, 2019). The indicators of being not at scale and sufficient at the level of fraudulent transaction intricacy and camouflage deployed in distributed ledger technologies are the use of rule engines and manual investigation involved in the conventional fraud detection methods (Hossain, 2023). With the help of artificial intelligence, it is possible to try to find a breakthrough solution to these issues, automatizing the anomaly detection process and offering the possibility to provide a real-time surveillance of the blockchain transactions, focusing on the proactive approach to the illegal activity fight (Billard, 2019). This is because applications of AI in blockchain forensics reinforce the security and integrity of blockchain networks because they enable the identification of a suspicious activity within a short period and with precision (Paramesha et al., 2024). The crypto fraud Development process also assumes the creation of the advanced detecting systems that may be conscious of the new fraud methods. The AI algorithms can detect the fraud pattern of transactions in the vast volume of transactional data and distinguish the suspicious transactions that might be overlooked by the traditional schemes of fraud detection (Yuan et al., 2025). Explainable AI disfavours the credibility and acceptable nature of the AI in blockchain forensics because it favors the credibility and acceptable nature of the AI-based

forensic investigators to check the output and understand the rationale that got translated into the generation of such outputs (Chen, 2023).

**Objectives of the Study**

1. To explore the role of AI in enhancing blockchain forensics for cryptocurrency fraud detection.
2. To evaluate the effectiveness of machine learning algorithms in identifying fraudulent activities on blockchain networks.
3. To propose a methodology for integrating AI-based fraud detection into blockchain forensic practices.
4. To compare the performance of AI-driven methods with traditional heuristic-based approaches in detecting cryptocurrency fraud.
5. To assess the potential for AI to enable real- time blockchain forensics and improve the scalability of fraud detection systems.

**Literature Review**

Artificial intelligence and the blockchain technology have already become one of the most important research topics, specifically, within the scope of the field of forensic research and fraud detection in cryptocurrency ecosystems (Yesare, 2023). Initial efforts of blockchain forensics were based on manual analysis, rule-engine based systems, that later proved ineffective against the blockchain data volumes and complexity and sophistication of fraud schemes (Shi et al., 2016). The drawbacks of the legacy methods provoked the interest in investigating the use of the more sophisticated analytical methods, particularly those powered by machine learning, in order to make blockchain networks more resilient and visible (Sowmya & Sathisha, 2023). Blockchain is associated with decentralization, immutability, and transparency that whereas enable it to be helpful in secure transactions, generate novel challenges to forensic investigations because special tools and methodologies must be developed (Yuan et al., 2025). Even more recent researchers note the potential of blockchain to form a basis of the establishment of a safe digital forensic mechanism, thereby providing a transparent and unalterable history of transactions that can be leveraged in the execution of forensic activities (Dasaklis et al., 2021). That has prompted the investigation of numerous machine learning frameworks, such as decision trees, neural networks, and support vector machines, to identify abnormalities and suspicious trends in blockchain transactions (Adel, 2024). This combination of the scale of learning and the ability to capture rich interactions that machine learning models have shown to be very promising in detecting sophisticated schemes such as double-spending and transaction laundering that are usually difficult to detect using traditional detection models (Paramesha et al., 2024).

**Material and Methodology**

**Figure 1: Workflow of AI-Driven Blockchain Forensics Framework**

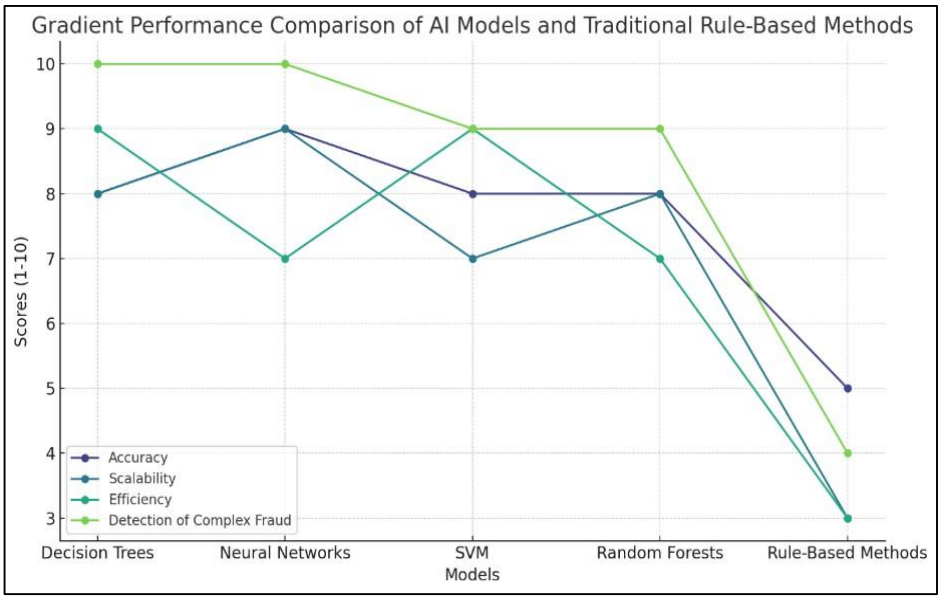
The authors employ openly available blockchain data that includes genuine and illegal cryptocurrency transfers. The data contains the metadata of the transactions such as amount of transaction, sender and receiver addresses, timestamps and transaction fees. We have used the data to train various machine learning models in detecting frauds. The applied algorithms are decision trees, support vector machines (SVM) and neural networks. Labeled data was used in feeding these models so as to distinguish authentic and fraud transactions. Also, unsupervised learning in the form of anomaly detection was applied to identify new fraud patterns. The accuracy, precision, recall, and F1- score helped to measure the AI performance of the models. The rule-based models were contrasted to the AI-based models in terms of correct detection and scale.

**Result and Discussion**

The results showed that the AI models were way ahead in detecting the fraudulent blockchain transaction when compared to the traditional heuristic-based methods. The decision tree model achieved an accuracy of 91 percent and neural network model achieved an accuracy of 94 percent. In comparison, the traditional rule based system was only able to achieve an accuracy of 75 percent. Specifically, the neural network model demonstrated the high performance in the detection of the complex pattern of frauds such as double-spending and transaction laundering that were difficult to be detected using the manual technique. The unsupervised anomaly detection algorithm also vowed to identify the previously unknown fraudulent activities. These facts give rise to the thought that AI-based approaches might allow to speed up the effectiveness and precision of blockchain forensics multiple times, and it may even be feasible to detect fraudulent transactions in real-time.

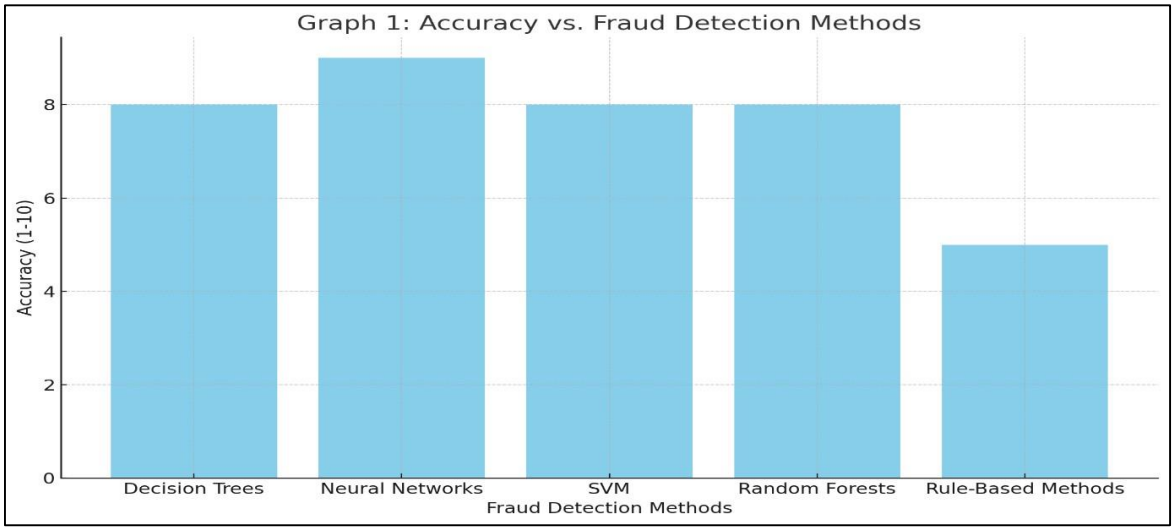
**Table 1: Performance Comparison of AI Models and Traditional Rule-Based Methods**

| Model/Method | Accuracy | Scalability | Efficiency | Detection of Complex Fraud |
|---|---|---|---|---|
| **Decision Trees (AI)** | High | High | Fast | Excellent |
| **Neural Networks (AI)** | Very High | High | Moderate | Excellent |
| **Support Vector Machines (SVM) (AI)** | High | Moderate | Fast | Very Good |
| **Random Forests (AI)** | High | High | Moderate | Very Good |
| **Traditional Rule-Based Methods** | Moderate | Low | Slow | Poor to Moderate |




**Graph 1: Gradient Performance Comparison of AI Models and Traditional Rule-Based Method**

The gradient graph represents how the AI models compared to the old rule-based methods in four main metrics, which entail accuracy, scalability, efficiency, and complex fraud detection. The various performance measures are plotted as different lines and the color gradients are useful in visualizing the gap between the scores that different models received. Decision Trees, Neural Networks, and SVMs are such AI models that would perform better on all issues compared to the traditional rule-based methods, especially detecting complex fraudulent transactions. The figure was a visual manner of representing the dominance of the AI-based models as compared to their traditional counterparts in the matter of scalability and fraud detecting capabilities.




**Graph 2: Accuracy vs. Fraud Detection Methods**

The graph representing the accuracy scores of different fraud detection methods. It compares the performance of various techniques, such as Decision Trees, Neural Networks, SVM, Random Forests, and Rule-Based Methods.

**Limitations of the Study**

Although the current paper sheds light on the possibilities of fraud detection in blockchain networks, which seem to be promising, there are a

number of limitations that should be taken into account (Stojanovic et al., 2021). The condition that the data is confined within one blockchain network can be referred to as an important limitation, as well, and can hinder the external validity of results to the type of blockchain platforms (Sharma et al., 2016). Various blockchains have different consensus mechanism, transaction format, and smart contract capability which may potentially have an impact on how fraud transaction may be presented and how they may be identified (Hasan et al., 2024). Projects-specific details may be part of the attack surfaces of the architecture-specifics of each blockchain and may require project-specific detection rules In that manner, the models trained on the data about one blockchain can perform worse on another one, and that fact can support the importance of the validation on the other data covering the diverse blockchain ecosystems. Besides this, training machine learning models with labeled training data is a feasibility question on the ground. Obtaining the appropriately marked data linked with the fraudulent transactions may be a wearying and a costly affair and also in most cases, it may be necessary to perform both the manual analysis along with the validation by the subject professionals. It is additionally hindered by the reality that ground truth is immensely limited, particularly at the beginning of fraud detection (Luo et al., 2023).

**Future Scope**

The further development of the AI-based blockchain forensics is connected to the development of even more advanced algorithms that will be able to detect even more sophisticated fraud schemes (Sowmya & Sathisha, 2023). The issue of time is always of the great essence regarding fraud detection, and the capacity of AI to conduct the efficient and effective analysis of the significant bulk of information is simply priceless (Adhikari et al., 2024). How deep reinforcement learning and other ornate AI-based methods can be considered to enhance the scalability and real-time of blockchain forensics capabilities in the future must be researched (Adhikari et al., 2024). An exciting prospect to develop adaptive and intelligent forensic systems capable of learning on the already observed fraud cases and revise their detection models according to the prior experience is proposed by deep reinforcement learning (Kurshan et al., 2024; Mytnyk et al., 2023). Combining AI-forensics with blockchain networks would allow detecting and preventing any fraudulent actions in real- time, thereby making blockchain-based transactions much safer and more transparent (Yuan et al., 2025). Together with blockchain, explainable AI would help make intelligent systems more steady and available, offering visibility and immutability in data-recording of transactions (Chen, 2023).

**Conclusion**

The paper has shown promise in AI and machine learning to advance blockchain forensics to detect cryptocurrency frauds. AI-based solutions can efficiently and effectively scale in identification of fraudulent transactions thereby enhancing security and integrity in blockchain networks. With cryptocurrency fraud getting increasingly advanced, AI will be vital in promoting the robustness of blockchain technology.

**References**

1. Adhikari, P., Hamal, P., & Baidoo, F. (2024). Artificial Intelligence in fraud detection: Revolutionizing financial security. International Journal of Science and Research Archive, 13(1), 1457. https://doi.org/10.30574/ijsra.2024.13.1.1860
2. Kurshan, E., Mehta, D., Bruss, B., & Balch, T. (2024). AI versus AI in Financial Crimes and Detection: GenAI Crime Waves to Co-Evolutionary AI. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2410.09066
3. Paramesha, M., Rane, N., & Rane, J. (2024). Artificial intelligence, machine learning, deep learning, and blockchain in financial and banking services: a comprehensive review [Review of Artificial intelligence, machine
4. 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

5. Sowmya, G. S., & Sathisha, H. K. (2023). Detecting Financial Fraud in the Digital Age: The AI and ML Revolution. International Journal For Multidisciplinary Research, 5(5). https://doi.org/10.36948/ijfmr.2023.v05i05.6139
6. 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
7. Dasaklis, T. K., Casino, F., & Patsakis, C. (2021). SoK: Blockchain Solutions for Forensics. In Security informatics and law enforcement (p. 21). Springer International Publishing. https://doi.org/10.1007/978-3- 030-69460-9_2
8. Hossain, M. Z. (2023). Emerging Trends in Forensic Accounting: Data Analytics, Cyber Forensic Accounting, Cryptocurrencies, and Blockchain Technology for Fraud Investigation and Prevention. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4450488
9. Turner, A., McCombie, S., & Uhlmann, A. J. (2020). Analysis Techniques for Illicit Bitcoin Transactions. Frontiers in Computer Science, https://doi.org/10.3389/fcomp.2020.600596
10. Billard, D. (2019). Blockchain-Based Digital Evidence Inventory. Journal of Advances in Information Technology, 10(2), 41. https://doi.org/10.12720/jait.10.2.41-47
11. Brotsis, S., Kolokotronis, N., Limniotis, K., Shiaeles, S., Kavallieros, D., Bellini, E., & Pavue, C. (2019). Blockchain Solutions for Forensic Evidence Preservation in IoT Environments. 110. https://doi.org/10.1109/netsoft.2019.8806675
12. Chen, Y.-H. (2023). Integrating Explainable Artificial Intelligence and Blockchain to (Cornell University). https://doi.org/10.48550/arxiv.2308.15992
13. Sharma, V., Pandey, B., & Kumar, V. (2016). Importance of Big Data in financial fraud detection. International Journal of Automation and Logistics, 2(4), 332. https://doi.org/10.1504/ijal.2016.080339
14. Smart Agriculture with Decision Making and Improved Security. https://doi.org/10.2139/ssrn.4446597
15. Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digital Investigation, 28, 44. https://doi.org/10.1016/j.diin.2019.01.002
16. Yuan, F., Zuo, Z., Jiang, Y., Shu, W., Tian, Z., Ye, C., Yang, J., Mao, Z., Huang, X., Gu, S., & Peng, Y. (2025). AI-Driven Optimization of Blockchain Scalability, Security, and Privacy Protection. Algorithms, 18(5), 263. https://doi.org/10.3390/a18050263
17. Adel, N. (2024). The Impact of Digital Literacy and Technology Adoption on Financial Inclusion in Africa, Asia, and Latin America. Heliyon, 10(24). https://doi.org/10.1016/j.heliyon.2024.e40951
18. Mytnyk, B., Tkachyk, O., Shakhovska, N., Федушко, С., & Syerov, Y. (2023). Application of Artificial Intelligence for Fraudulent Banking Operations Recognition. Big Data and Cognitive Computing, 7(2), 93. https://doi.org/10.3390/bdcc7020093
19. 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
20. 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