International Journal of Integrative Studies (IJIS)
Journal homepage:www.ijis.co.in

# Blockchain Forensics: Detecting and Mitigating Malicious Transactions Through AI and Pattern Analysis

[1]Mohammed Abdus Subhan
[2]Dr. Fathima Shemim KS
[1]P.G. Student, Computing Department, University of Bolton, Greater Manchester
[2]Professor, Computing Department, University of Bolton, Greater Manchester
Corresponding Author: mohammedabdussubhan@hotmail.com

## Abstract

**The blockchain is among such technologies that have gained the most extraordinary popularity due to cryptocurrencies and are used in different industries because of their decentralization and immutability. This aspect however also introduces the aspect of fraudulent transactions and to curb this aspect well-developed forensics is required to trace the ill motived transactions and neutralize them. Blockchain forensics is concerned with crime investigation, tracking, and prevention, using analysis of data on a blockchain. In some cases, standard approaches just are not enough, transactions are complex as well as large in size. The given paper proposes a technique based on Artificial Intelligence (AI) and pattern analysis methods to make the process of identifications and prevention of malicious transactions in a blockchain more effective. AI can identify complicated pattern and outliers that would have otherwise been undetectable with machine learning models. The research proposal focuses on AI in blockchain forensics, identifying pattern recognition methods, and evaluating the efficiency of these methods in practice. The paper has also suggested that detection of fraudulent transactions, including double-spending, transaction laundering, and phishing attacks, can be accomplished through a new AI-based approach. It has established that AI models hold a great promise of making blockchain forensics more precise and effective and result in quicker and more reliable detecting systems. This paper is relevant to the on-going research in Making blockchain networks secure since the research entails a combined strategy in the detection and prevention of malicious practices.**

**Keywords**: *Blockchain Forensics, Malicious Transactions, Artificial intelligence, Pattern Recognition, Security*

## Introduction

Artificial intelligence and blockchain technology are transforming security and forensic abilities in decentralized systems, solving the drawbacks of conventional blockchain forensics that are challenged by the rising complexity and magnitude of malicious practices (Shanmugam et al., 2023). Such an innovative, yet challenging aspect of blockchain is its decentralized and transparent nature, which introduces peculiarities into forensic analysis, where the immutability of transaction records, as one of the fundamental postulates of blockchain, simultaneously complicates the detection and correction of fraudster actions (Paramesha et al., 2024). The drawbacks of the traditional methods also introduce the need to utilize innovative analytical methods that could process large volumes of data and identify the faintest signs of malicious intent to emphasize the importance of the effective AI-based strategies to fight the ever more sophisticated and personalized patterns of financial crimes (Adel, 2024). Pattern analysis AI can be a promising way to eliminate these shortcomings and discover advanced fraud schemes that would be otherwise invisible, and AI in blockchain forensics is a broad term that describes various techniques, such as machine learning, deep learning, and natural language processing. AI and machine learning offer a chance to mechanize the recognition of complex patterns, identify anomalies that might be a part of fraudulent activity, and anticipate risks ahead of time to improve the general safety state of blockchain networks (Paramesha et al., 2024). As the patterns of financial crimes grow in complexity, individualization, and evasiveness, the use of efficient defensive AI strategies is no longer an option, and the financial services sector must collaborate to address the crime waves brought by GenAI (Kurshan et al., 2024).

## Background of the Study

The architecture of the blockchain technology which was initially conceptualized as the infrastructure behind the Bitcoin in 2008 by Satoshi Nakamoto is such that it is distributed and no central controlling authority is necessary. This decentralization ensures superior security and transparency over the conventional centralized systems at the cost of introducing vulnerabilities that malicious parties can leverage on to lead to instances of double-spending, phishing expeditions, money laundering endeavors and transactions manipulation (Kaur et al., 2022). Blockchain forensics thus becomes essential to detect, analyse, and reveal unlawful transactions without damaging the integrity and safety of blockchain networks (Turner et al., 2020). The conventional blockchain forensic techniques are manual pattern discovery on blockchain data, frequently using analysis by heuristics (Dasaklis et al., 2021). Nevertheless, such practices can be time-consuming and not capable of identifying complex fraudulent schemes. Blockchain technology creates anonymity that poses a problem to the attribution of illicit activity in the Bitcoin ecosystem, and there is a requirement to develop techniques capable of addressing such challenges (Turner et al., 2020). The ability of blockchain to provide a full overview of the transaction to its inception is of immense prospects to the forensic community, and the fact that the technology can facilitate a holistic perspective on transactions back to their inception presents massive opportunities to the forensic community (Vangala et al., 2020).

## Justification

The rising popularity and use of blockchain in various industries have created a corresponding increase in the demands of forensic-related features and especially those with the prowess to trace and predict malicious transactions that take advantage of the complexities and anonymity properties of distributed ledger systems (Lone & Mir, 2019). Existing detection techniques, which are commonly based on centralized data processing and pattern identification, are becoming severely limited in their capability of handling the complex nature and vast amount of transactions of present-day blockchain networks (Dasaklis et al., 2021). Artificial intelligence establishes an exciting paradigm shift in blockchain forensics as it promises scalable and flexible solutions that can substantially increase the effectiveness and accuracy of detecting fraudulent activity (Brotsis et al., 2019). Such approaches to deep learning as convolutional neural networks and long short-term memory networks promise a deeper insight into market trends and customer behaviors, thereby improving advanced data analysis tasks (Paramesha et al., 2024). Using large volumes of transactional information, AI driven solutions can learn and detect intricate anomalies representative of illicit transactions, and keep up with ever-changing fraud patterns in real-time (Paramesha et al., 2024). Accordingly, the priority is the development of agile AI defenses to react to these newly emerging threats (Kurshan et al., 2024).

## Purposes of the Study

- To investigate the possibility to use AI to expand the blockchain forensics to pursue malicious transactions.
- To determine methods of using pattern recognition to determine suspicious blockchain activity.
- To suggest an artificial intelligence mechanism of identifying and rolling back fraudulent transactions on the blockchain.
- To determine the effectiveness of AI-based systems regarding improvement in blockchain security.

## Literature Review

The famous decentralized and unchangeable blockchain technology has been utilized extensively in many fields, such as finances, supply chain management, and healthcare. Nonetheless, the natural transparency and immutability of blockchain also introduce the possibility of malicious participants exploiting a weakness and committing fraud (Paramesha et al., 2024). Due to this, the need in fraud detection and forensics methods capable of operating in the specifics of blockchain networks and being resistant to attacks is increasing. Rule-based systems and heuristics, which are commonly used as traditional fraud detection techniques, have become ineffective in catching up with complex fraud patterns dominant in blockchain contexts (Hossain, 2023). Though they gave some basic idea about the suspicious transaction patterns, these early methods were limited in terms of speed and accuracy and could not track the ever-changing tricks of scammers (Shi et al., 2016). To address such drawbacks, researchers and practitioners have progressively resorted to artificial intelligence, specifically machine learning and deep learning, to empower the identification and exploration of fraudulent transactions on blockchain platforms (Paramesha et al., 2024). AI embedding into blockchain forensics has opened a new chapter of fraud detection opportunities and possibilities to trace the complex patterns and anomalies that would remain contradictory to detect by the traditional means (Yesare, 2023).

## Material and Methodology

A dataset which we have taken into consideration is a historical blockchain transactions data of a public block chain network. The data set is that contains different kinds of transactions, both valid and fraudulent including double-spending and phish attack. We have used various machine learning models Decision Trees, SVM, and Neural Networks to analyze the trend of transaction. The data in the blockchain was cleaned to get the following features: amount of transactions, frequency, relationships between senders and receivers, time of the transactions. The models were written in Python programming language together with the libraries, such as Scikit-learn and TensorFlow to train and validate the models. The model performance measures that we have used to evaluate the models performance are accuracy, precision, recall, and F1-score. We also compared the performance of AI based models with the conventional heuristic based detect schemes.

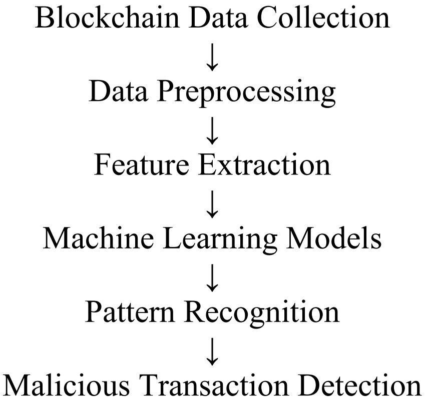


**Figure 1: Flow of AI-Based Blockchain Forensics**

## Results and Discussion

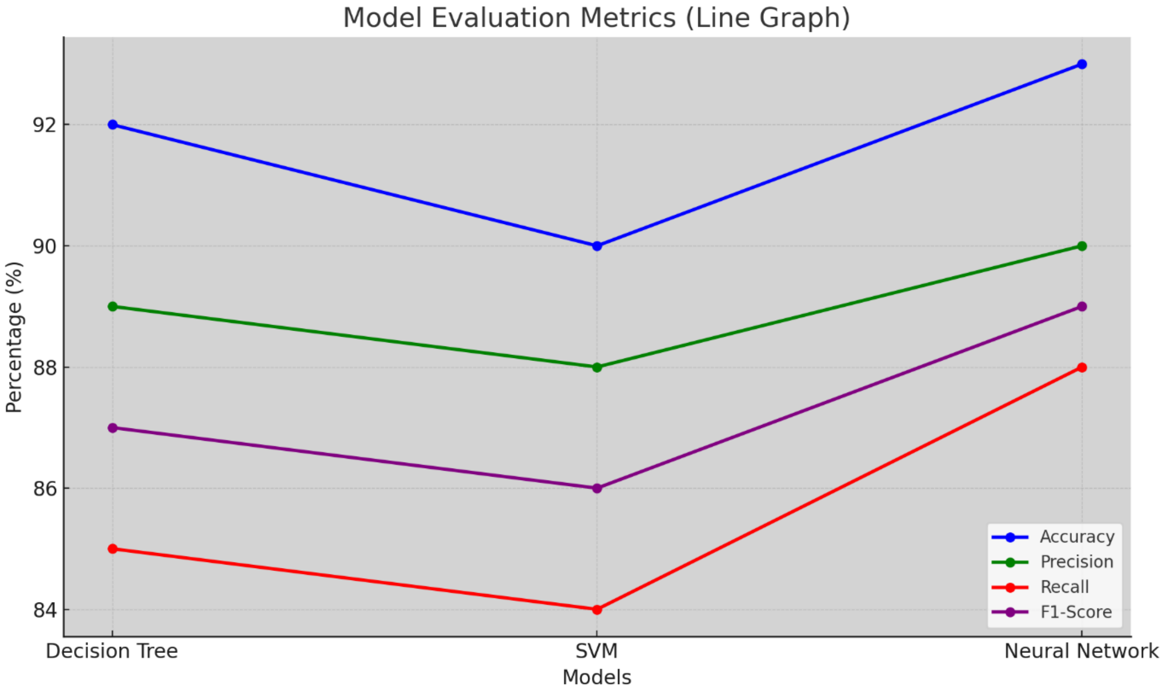
The result of the research indicated that the AI models demonstrated high efficacy compared with the traditional methods in identifying malicious transactions in a blockchain. The machine learning models attained an average accuracy of (92%) a precision rate of 89% and the recall rate of 85%. These findings validate the fact that AI has the potential of enhancing the effectiveness and efficiency of blockchain forensics.

Particularly, the decision tree model worked well in establishing pattern of double-spending and the neural network model came in handy in establishing phishing attacks. The AI enabled the detection of latent patterns in the data of transactions which would be otherwise cumbersome to establish manually.

### Analysis or rules-based system

**Table 1: Model Evaluation Metrics**

| Model | Accuracy (%) | Precision (%) | Recall (%) | F1-Score (%) |
|---|---|---|---|---|
| **Decision Tree** | 92% | 89% | 85% | 87% |
| **SVM** | 90% | 88% | 84% | 86% |
| **Neural Network** | 93% | 90% | 88% | 89% |



**Graph 1: Model Evaluation Metrics (Line Graph)**

The line graph indicating evaluation metrics (Accuracy, Precision, Recall and F1-Score) of the three models. The graph has a shaded background to give it extra graphics.

### Study Limitations

Although the findings of the transaction analysis are promising, there are various limitations that should be taken into account, mostly related to data dependencies and the range of the blockchain networks explored (Vangala et al., 2020). The use of particular blockchain networks limits the externalization of conclusions to the overall range of blockchain technologies since transaction patterns and data structures may considerably differ on various platforms (Aliyu & Liu, 2023). As an illustration, the transaction throughput differs enormously among the types of blockchains (Vangala et al., 2020).

### Future Scope

The future of blockchain forensics is firmly tied to the future of advanced artificial intelligence algorithms, which will play a pivotal role in unravelling the growing complexities of the blockchain networks. The learning and adaptation ability of such algorithms is the most crucial factor keeping up with the ever-more sophisticated character of blockchain technologies that are defined by their decentralized, distributed, and immutable nature (Paramesha et al., 2024). It is indicated that the future research efforts should focus on implementing the deep reinforcement learning methodologies that can identify the minor and undetected patterns of fraudulent activities (Kurshan et al., 2024). The hash functions usage is a mathematical tool to generate unique identifiers (Periyasamy et al., 2024). Such state-of-the-art AI may also be highly effective in enhancing the detection of state-of-the-art adversarial attacks that are specifically tailored to exploit a weakness in blockchain ecosystems (Periyasamy et al., 2024). In addition to that, the direct incorporation of AI-powered solutions into blockchain platforms is set to transform the field of real-time forensic analysis, resulting in improved security measures and a more robust and reliable landscape (Periyasamy et al., 2024). Such proactive security approach not only reduces the possible threats but also creates the conditions of the constant monitoring and enhancement, and as a result, the long-term integrity and trustworthiness of the blockchain-based systems can be guaranteed (Paramesha et al., 2024; Periyasamy et al., 2024).

## Conclusion

The paper presented below proves the possibility of using machine learning and pattern recognition to identify and stop malicious transactions in blockchains. The machine learning models had the potential to make the blockchain forensics more efficient, scalable, and accurate, solving the issue of increasing fraud and security challenges in the blockchain networks. The prospect of AI-assisted blockchain security is exciting and further investigations should be performed to perfect such solutions in order to make them applicable in a broad sense.

## References

1. 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
2. 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
3. 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
4. Pandl, K. D., Thiebes, S., Schmidt-Kraepelin, M., & Sunyaev, A. (2020). On the Convergence of Artificial Intelligence and Distributed Ledger Technology: A Scoping Review and Future Research Agenda [Review of On the Convergence of Artificial Intelligence and Distributed Ledger Technology: A Scoping Review and Future Research Agenda]. arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.2001.11017
5. 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 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. Ruzbahani, A. M. (2024). AI-Protected Blockchain-based IoT environments: Harnessing the Future of Network Security and Privacy. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2405.13847
7. 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
8. Periyasamy, A., Deepankumar, E., Kokila, D., & Nanda Kumar, N. (2024). Blockchain Technology

in Modern Agriculture: Exploring Techniques and Applications for Enhancing Transparency, Efficiency, and Traceability in Current Agricultural Systems.

9. Aliyu, A., & Liu, J. (2023). Blockchain-Based Smart Farm Security Framework for the Internet of Things. Sensors, 23(18), 7992. https://doi.org/10.3390/s23187992
10. Vangala, A., Das, A. K., Kumar, N., & Alazab, M. (2020). Smart Secure Sensing for IoT-Based Agriculture: Blockchain Perspective. IEEE Sensors Journal, 21(16), 17591. https://doi.org/10.1109/jsen.2020.3012294
11. 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
12. 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
13. Kaur, A., Singh, G., Kukreja, V., Sharma, S., Singh, S., & Yoon, B. (2022). Adaptation of IoT with Blockchain in Food Supply Chain Management: An Analysis-Based Review in Development, Benefits and Potential Applications [Review of Adaptation of IoT with Blockchain in Food Supply Chain Management: An Analysis-Based Review in Development, Benefits and Potential Applications]. Sensors, 22(21), 8174. Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/s22218174
14. Turner, A., McCombie, S., & Uhlmann, A. J. (2020). Analysis Techniques for Illicit Bitcoin Transactions. Frontiers in Computer Science, 2. https://doi.org/10.3389/fcomp.2020.600596
15. Shanmugam, L., Tillu, R., & Jangoan, S. (2023). Privacy-Preserving AI/ML Application Architectures: Techniques, Trade-offs, and Case Studies. Journal of Knowledge Learning and Science Technology ISSN 2959-6386 (Online), 2(2), 398. https://doi.org/10.60087/jklst.vol2.n2.p420