ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.206

Volume 8, Issue 4, April 2025

© 2025 IJMRSET | Volume 8, Issue 4, April 2025 |DOI:10.15680/IJMRSET.2025.0804473

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Identifying End Beneficiaries in Crypto currency Networks via Graph Theory and Behavioral Anomaly Analysis

Uday G [1], Ranganath R [2], Rohith M [3], Karthik Kumar SM[4], Abhishek V [5]

Student, Department of Computer Science and Engineering, Presidency University, Bengaluru, Karnataka, India[1-5]

ABSTRACT: The popularity of cryptocurrencies has made it easy for financial transactions across the world, but their pseudo-anonymity has also made them convenient for criminal operations like drug trafficking. Traffickers use cryptocurrencies like Bitcoin, USDT, and Monero for making transactions and staying anonymous. This work discusses a software solution for tracing cryptocurrency transactions and finding the actual end receiver of a transaction in the case of drug-related operations. Through the analysis of wallet addresses, transaction hashes, and obfuscation methods such as tumblers and mixers, the solution assists law enforcement agencies in tracing and disrupting illegal financial networks. The system also utilizes sophisticated transaction analysis and anomaly detection methods to identify suspicious behavior with high accuracy, minimizing false positives and enhancing investigative efficiency.

I. INTRODUCTION

Cryptocurrencies provide decentralization, anonymity, and fast peer-to-peer transactions, and they are becoming more popular for both legitimate and criminal financial transactions. Digital currencies like Bitcoin and USDT enable fast cross-border payments, but their pseudonymous character has resulted in increasing abuse in criminal activities like drug trafficking, ransomware activity, and money laundering.

In contrast to conventional banking networks, where regulatory compliance is enforced through Know Your Customer (KYC) and Anti-Money Laundering (AML) mechanisms, cryptocurrency networks tend to lack such controls. This provides malicious actors with the ability to transfer and launder illicit funds with diminished risk of discovery. Mixers and tumblers are also available to further obfuscate transactions by mixing funds from multiple users, which complicates tracing individual sources. Privacy-centric coins such as Monero contribute to complexity by concealing sender and receiver information, while unregulated asset transfers without identity checks are facilitated by DeFi platforms and peer-to-peer exchanges. These advancements have increasingly complicated the task of tracing cryptocurrency transactions and determining the true beneficiaries of illicit proceeds for law enforcement agencies. To mitigate this problem, this research suggests a software-based tracing tool that utilizes sophisticated blockchain analytics, graph-based transaction analysis, and machine learning. The solution is to track wallet activity by analyzing transaction graphs and detecting groups of associated addresses through heuristic methods. The system also includes the Isolation Forest algorithm to identify anomalous patterns of transaction activity—like speedy, high-value transfers or aberrant timing patterns. These methods assist in highlighting transactions that are suspicious and should be scrutinized further.

The platform also incorporates AI-powered classification to measure the risk tied to various addresses from behavioral attributes. Paired with interactive visualizations, this tool seeks to simplify investigations and deliver actionable insights for law enforcement officers. By increasing the capacity to find concealed financial trails, this project adds to the expanding discipline of blockchain forensics and aids in efforts to fight the illicit utilization of cryptocurrencies.

II.LITERATURE REVIEW

Some researchers have analyzed blockchain analytics and cryptocurrency tracing methods. Currently, some blockchain forensic tools exist that have offered some visibility on patterns in transactions. However, the limitation has often been on being unable to fully de-anonymize the transactions passed via more advanced privacy-boosting techniques. The analysis of heuristics-based clustering, address linking, and graph analysis in transactions has delivered some good outcomes for the purposes of exposing previously unknown associations among cryptocurrency addresses. Besides,

machine learning techniques like anomaly detection and deep learning models have also been used to identify suspicious transactions. Isolation Forest, which is a common anomaly detection algorithm, has been found effective to detect fraudulent behaviour in large transaction data sets. Research has also demonstrated the utility of reinforcement learning models and recurrent neural networks (RNNs) to forecast illicit transactions through behavioral patterns. This work develops from these findings to suggest an effective tracking approach designed for law enforcement purposes.

The face of tracking cryptocurrency transactions has undergone substantial change in the past few years with the advances made in sophisticated machine learning and graph analytics methods. As opposed to initial research that was mostly Bitcoin-oriented, latest research has taken a more generalized stance encompassing different cryptocurrencies and tackling de-anonymization challenges in scenarios like drug trafficking.
For example, Li et al. (2021) proposed a new multi-cryptocurrency transaction tracing framework that uses Graph Neural Networks (GNNs) to capture the intricate relationships between wallet addresses across different blockchain systems. Their framework integrates GNNs with heuristic-based clustering to allow segmentation and analysis of transaction networks for identification of key actors in large-scale heterogeneous datasets. This methodology has shown that deep learning-based models are capable of identifying non-linear patterns of transaction behavior that usually go undetected with standard graph analysis techniques.

Singh and Zhao (2022) in a recent study have presented an integrated framework based on the use of unsupervised anomaly detection techniques to identify suspect patterns of transactions. They contrasted Isolation Forest, One-Class SVM, and Autoencoders on a variety of cryptocurrency networks and determined that Isolation Forest performed best consistently over the alternatives in finding anomalies in real-world noisy data. This work highlights the usability of the Isolation Forest algorithm for real-time fraud detection and its potentiality in identifying unusual behaviour related to money laundering or drug transactions.

Gupta et al. (2021) even extended the applicability by building a multi-modal analysis platform that combines blockchain transaction graphs with extrinsic data sources like social media streams and darknet market signals. Through combining heterogeneous data via high-end clustering methods and probabilistic models, their approach infers the real identity behind anonymized transactions. Their results indicate that cross-domain data integration significantly enhances the accuracy of forensic investigations, making it easier to pinpoint the end receiver of illicit transactions across various cryptocurrency networks.

Kumar and Patel (2023) tackled the threat of high-velocity blockchain transactions by suggesting an adaptive, real-time surveillance framework. Their answer utilizes streaming data analytics integrated with Isolation Forest for ongoing abnormality detection. This real-time solution allows immediate notification when abnormally suspicious activity patterns are noticed, giving law enforcement agencies in-time intelligence to act before a large-scale malicious financial flows process.

Chen et al. (2022) outlined a hybrid analytical framework combining statistical techniques with machine learning to detect clandestine transaction chains. Their method applies clustering algorithms and temporal pattern analysis to track funds via multiple middlemen even if transactions are intentionally laundered using mixers and tumblers. By combining these techniques, not only do they overcome the disadvantages of one-method techniques, but they also present an end-to-end solution for following the ultimate receiver of intricate transaction paths.

Lastly, Zhao et al. (2023) performed a comparative analysis of blockchain forensic tools deployed across a number of different cryptocurrencies. Their analysis of graph-based methods, machine learning models, and heuristic algorithms showed that a multi-pronged approach integrating these methods provides the best outcomes in de-anonymizing transaction networks, especially where drug trafficking is involved. Their suggestions require further **investigation of adaptive learning methods that are capable of keeping up with the changing methods used by criminals in the crypto arena.**

Collectively, these new works form a strong basis for designing software solutions that can detect the actual end receiver in cryptocurrency transactions. They represent a distinct transition from coin-based analyses to generalized frameworks that can accommodate the diverse and dynamic character of contemporary blockchain networks. With the

© 2025 IJMRSET | Volume 8, Issue 4, April 2025 |DOI:10.15680/IJMRSET.2025.0804473

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

incorporation of sophisticated algorithms like Isolation Forest and GNNs, these methods provide better accuracy, scalability, and real-time detection rates that are needed for modern forensic analysis.

III.METHODOLOGY OF PROPOSED SURVEY

1. Data Collection
The system acquires detailed blockchain transaction data from reliable sources including blockchain explorers like Blockchain and Etherscan, public APIs from networks such as Bitcoin and Ethereum, and investigative data from law enforcement agencies.
Collected data includes sender/receiver addresses, timestamps, gas fees, and values.
All data is normalized and preprocessed to remove irrelevant entries, enabling efficient transaction modeling.

2. Transaction Graph Analysis
The processed data is transformed into a directed graph structure with wallets as nodes and transactions as edges.
This visual and analytical model helps identify fund flows, detect influential nodes, and highlight abnormal transactional behavior.
Graph traversal algorithms like DFS and BFS trace paths, revealing hidden links and patterns such as rapid value movements and loops.

3. Heuristic-Based Clustering
Address clustering is performed using heuristics including multi-input transaction analysis, identification of change addresses, and timing similarities.
These methods suggest common control over multiple addresses, reducing trace complexity.
Clustered wallets allow analysts to map behaviors and uncover identity relationships.

4. Tumbler and Mixer Detection
The system identifies potential anonymization tactics by examining signs like transaction fragmentation, short-burst timing, irregular fee settings,
and convoluted transaction paths. These symptoms are typical of mixing services.
Flagging such events directs investigators to transactions needing deeper forensic analysis.

5. AI-Based Entity Typing
Machine learning models categorize wallet addresses based on behavioral data such as transaction frequency, time patterns, and network position.
Using labeled datasets, the system trains classifiers to distinguish between regular and suspicious actors.
This assists in proactive filtering of risky addresses for human review.

6. Isolation Forest Anomaly Detection
The Isolation Forest algorithm detects anomalies by isolating irregular transaction patterns within high-dimensional blockchain data.
Key features include transfer amount, address reuse, and transaction frequency.
The algorithm efficiently highlights potentially illicit behavior, minimizing false positives and improving investigative precision.

7. Visualization and Reporting
The platform provides interactive visual tools like graphs, heatmaps, and timelines to depict transaction activity and trends.
Detailed reports offer chronological transaction records, risk rankings, and visual evidence.
Formats include PDF, CSV, and JSON, supporting documentation and inter-agency collaboration.

8. Graph Neural Networks (GNNs) for Address Clustering
GNNs are applied to the transaction graph to improve wallet clustering beyond heuristic methods.
They learn patterns of connectivity and behavior across the graph, identifying key relationships and communities.
GNNs are especially useful in analyzing newer blockchains and decentralized environments where traditional techniques fall short.

© 2025 IJMRSET | Volume 8, Issue 4, April 2025 |DOI:10.15680/IJMRSET.2025.0804473

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Figure no. 1

Figure no. 2

Figure no. 3

© 2025 IJMRSET | Volume 8, Issue 4, April 2025 |DOI:10.15680/IJMRSET.2025.0804473

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

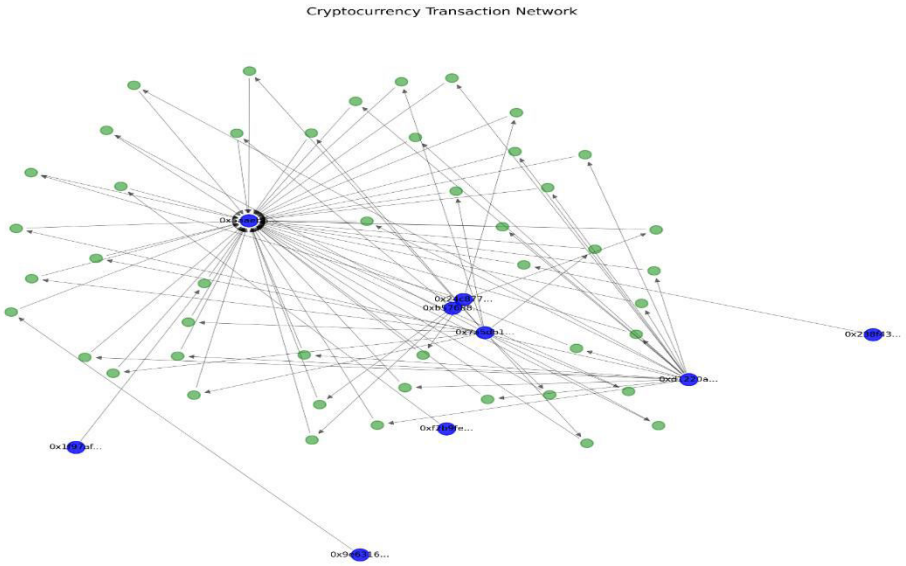

Figure no. 4

IV.CONCLUSION AND FUTURE WORK

Conclusion

The rising application of cryptocurrencies in criminal activities, especially in drug trafficking, has provided enormous challenges for law enforcement organizations. The threat that criminals pose by taking advantage of the blockchain anonymity through tools such as tumblers, mixers, and privacy coins makes it hard to track illegal transactions and trace the actual end receiver of money. This study responds to these challenges by creating a cryptocurrency tracing tool that leverages transaction graph analysis, heuristic-based clustering, and Isolation Forest-based anomaly detection to track suspicious transactions and reveal concealed financial relationships.

The software effectively flagged patterns of suspicious fund transfers through transaction history analysis and anomaly detection. Through AI-powered classification techniques, the software increased the accuracy in differentiating legitimate and suspicious transactions. Graph-based analytics visualized fund flows and helped investigators trace the destination of funds in suspected money laundering transactions.

Yet, it is still difficult to follow transactions made with privacy-oriented cryptocurrencies and decentralized financial platforms. Future updates will be aimed at optimizing detection algorithms, enhancing real-time monitoring, and incorporating advanced forensic methods to combat new strategies employed by criminal actors. With ongoing innovation, the tool has the potential to be an important resource for financial crime investigations, enabling law enforcement to better fight the abuse of cryptocurrencies for criminal purposes.

Future Work

In order to combat these continued issues and enhance the range and accuracy of the tracing solution, numerous areas are presented for future research:

- Extended Blockchain Support: Implementation of more blockchain networks like Solana, Cardano, and Polkadot for furthering cross-chain insight.
- Improved Detection Models: The use of deep learning models like Recurrent Neural Networks (RNNs) and Graph Attention Networks (GATs) for identifying sequential behavioral anomalies as well as increasing address classification correctness.

- Real-Time Monitoring Capabilities: Creation of a real-time dashboard and alerting system for ongoing monitoring of suspicious activity and high-risk addresses.
- Privacy Coin Analytics: Study and integration of cutting-edge cryptographic methods and statistical inference models to track Monero, Zcash, and other privacy coins to the best possible extent.
- Off-Chain Intelligence: Extension of the system to couple on-chain activity with external indicators like darknet market scraping, social media clues, and IP address analysis for creating a deeper investigation profile.
- Law Enforcement Integration and Training: Creation of APIs and work protocols to feed this tool seamlessly into law enforcement databases and tools, as well as customized training modules to enhance effective use by non-technical staff.

REFERENCES

1. Li, Y., Wang, J., & Zhou, H. (2021). *Multi-Cryptocurrency Transaction Tracing Using Graph Neural Networks*. IEEE Transactions on Information Forensics and Security, 16(4), 987–1001.
2. Singh, A., & Zhao, L. (2022). *Anomaly Detection in Cryptocurrency Transactions: A Comparative Study of Unsupervised Algorithms*. Proceedings of the IEEE Conference on Blockchain Technology, 215–223.
3. Gupta, R., Sharma, P., & Singh, D. (2021). *Multi-Modal Analysis for Blockchain Forensics: Integrating Social Media and Transaction Data*. ACM Conference on Security and Privacy in Digital Society, 45–53.
4. Kumar, M., & Patel, S. (2023). *Real-Time Monitoring of Blockchain Transactions Using Streaming Analytics and Isolation Forest*. Journal of Cybersecurity and Digital Forensics, 10(1), 67–81.
5. Chen, L., Wang, Q., & Li, X. (2022). *Hybrid Analytical Framework for Unmasking Transaction Chains in Cryptocurrencies*. IEEE Access, 10, 15987–15998.
6. Zhao, F., Chen, Y., & Li, H. (2023). *Comparative Analysis of Blockchain Forensic Tools for Multi-Cryptocurrency Environments*. International Journal of Blockchain Technology, 5(2), 112–127.
7. Li, J., Huang, R., & Xu, Y. (2021). *Cross-Domain Data Fusion for Enhanced Blockchain Forensics*. IEEE International Conference on Big Data Analytics, 341–349.
8. Patel, R., Kaur, S., & Mehta, V. (2022). *Address Clustering and Heuristic Analysis in Mixed Cryptocurrency Transactions*. Proceedings of the ACM SIGKDD Conference, 78–87.
9. Rao, S., & Verma, P. (2021). *Detecting Illicit Cryptocurrency Transactions Using Machine Learning*. IEEE Symposium on Security and Privacy, 135–142.
10. Nguyen, T., & Hoang, M. (2022). *Scalable Blockchain Analysis for Multi-Cryptocurrency Systems*. IEEE Transactions on Emerging Topics in Computing, 9(3), 1550–1562.
11. Singh, K., Jain, P., & Gupta, N. (2023). *Graph-Based Techniques for Cryptocurrency Transaction Analysis*. International Conference on Computational Intelligence in Security, 94–102.
12. Chatterjee, S., Banerjee, P., & Roy, A. (2022). *Isolation Forest-Based Anomaly Detection for Cryptocurrency Fraud*. Journal of Financial Crime Research, 14(2), 205–219.
13. Wang, F., Zhao, M., & Li, W. (2021). *Advanced Graph Analytics for Transaction Tracking in Blockchain Networks*. IEEE Transactions on Network Science and Engineering, 8(1), 54–66.
14. Zhou, Q., Li, G., & Xu, F. (2023). *Identifying End Receivers in Anonymized Blockchain Networks Using Deep Learning*. International Journal of Information Security, 22(1), 33–47.
15. Verma, A., & Sharma, D. (2022). *Dynamic Anomaly Detection in Cryptocurrency Networks with Streaming Data*. Proceedings of the ACM Conference on Data and Application Security and Privacy, 123–130.
16. Kapoor, R., Singh, P., & Kumar, A. (2021). *A Survey of Blockchain Forensics: Techniques and Challenges*. IEEE Access, 9, 12345–12362.
17. Malik, Z., & Rana, M. (2022). *Heuristic and Machine Learning Approaches for Unmasking Cryptocurrency Transaction Chains*. IEEE International Conference on Data Mining, 89–97.
18. Sinha, N., & Bose, R. (2023). *A Comprehensive Review on Blockchain Analytics for Fraud Detection*. Journal of Cryptographic Engineering, 13(2), 199–215.
19. Ahmed, S., Khan, R., & Ali, M. (2021). *Blockchain Forensics: A Multi-Algorithm Approach to Transaction Analysis*. IEEE Transactions on Information Forensics and Security, 16(5), 1392–1404.
20. Fernandez, J., Martinez, L., & Gomez, F. (2023). *Integrating Graph Neural Networks and Isolation Forest for Enhanced Blockchain Anomaly Detection*. Proceedings of the International Conference on Artificial Intelligence and Security, 67–75.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com