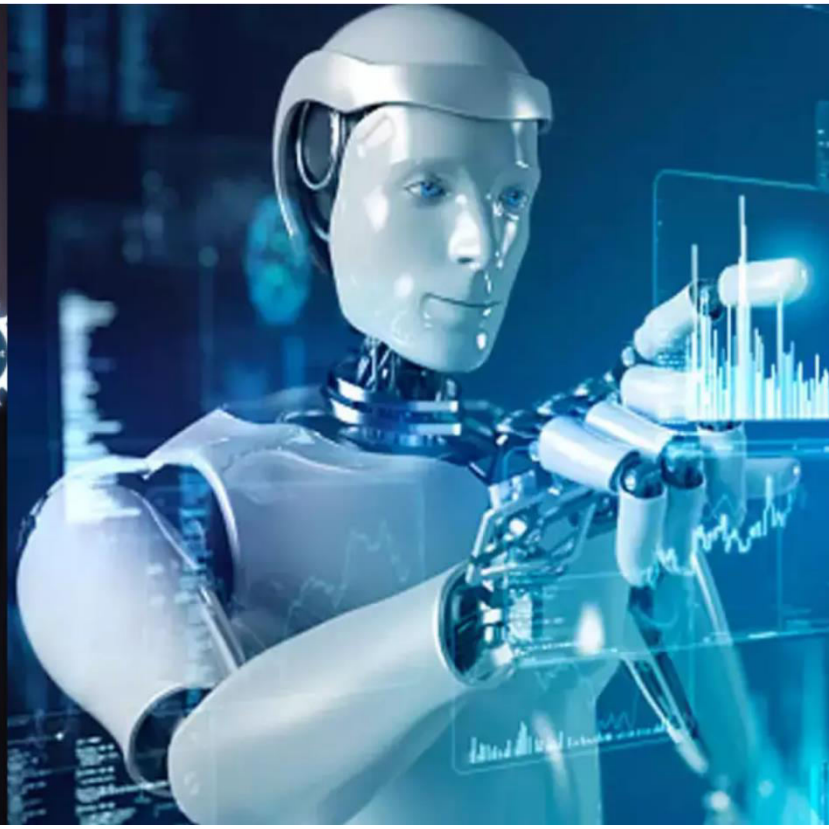
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

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



Impact Factor: 8.699

Volume 14, Issue 11, November 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411042|

AI-Based Tracing of Suspicious Cryptocurrency Transactions across Multiple Blockchains

Arjun Kadam[1], Sudhir Dongargave[2], Akash Chindhe[3], Prof.Gunjal.H.D[4]

Department of Computer Engineering, Vishwabharati Academy's College of Engineering, Ahmednagar, Maharashtra, India[1,2,3,4]

ABSTRACT: Cryptocurrencies have revolutionized digital finance by enabling decentralized and transparent transactions, but their pseudonymous nature has also made them a major tool for illicit activities such as money laundering, scams, and cyber theft. Traditional blockchain explorers provide only limited visibility, often confined to single-chain transaction tracking and manual investigation. This review focuses on the development and enhancement of an AI-based framework for tracing suspicious cryptocurrency transactions across multiple blockchains. The proposed system integrates data from blockchain analysis tools like Bitquery and Etherscan, applies machine learning and anomaly detection algorithms, and visualizes relationships using a Neo4j graph database. Through behavior-based pattern analysis, the system identifies fraudulent wallets and detects complex schemes such as chain-hopping, tumbling, and fund layering. The review also examines existing methods, their limitations, and the role of artificial intelligence in improving forensic blockchain analytics. The integration of multi-chain data aggregation, AI-based behavioral learning, and graph visualization significantly enhances transparency and provides law enforcement and regulatory bodies with a powerful tool for detecting and preventing financial cybercrime in decentralized ecosystems.

KEYWORDS: wallet address, flow of funds, Thief, Ethereum, Blockchain, etc

I. INTRODUCTION

In today's fast-paced automotive market, car buyers face an overwhelming array of choices, making the decision-making process more complex than ever. With numerous models, features, and price points to consider, consumers often struggle to find reliable information to help them make informed decisions. The Interactive Car Comparison Tool aims to simplify this process by providing an intuitive platform where users can compare different car models from various manufacturers side by side. This tool not only allows users to evaluate specifications, safety ratings, and user reviews but also incorporates advanced algorithms to predict the prices of used cars based on historical data and market trends.

Buyers today expect a seamless experience that integrates both technology and personalized information. The Interactive Car Comparison Tool addresses this need by leveraging modern web technologies to create a user-friendly interface that caters to diverse consumer preferences. By offering features like real-time comparisons and price predictions, the tool helps demystify the car buying process, making it easier for users to understand the value of their choices. This innovative approach not only enhances user engagement but also fosters informed decision-making, paving the way for a more satisfying and efficient car-buying journey.

II. LITERATURE SURVEY

1. "A Machine Learning Approach for Detecting Illicit Cryptocurrency Transactions"
Author: S. Weber et al., 2019 – IEEE Access
This study presents a supervised learning framework using transaction features such as amount, time, and frequency to detect suspicious cryptocurrency activities. Algorithms like Random Forest and XGBoost were used to classify transactions as illicit or legitimate, achieving improved detection accuracy.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411042|

2. "Characterizing Ethereum Scams Using Transaction Graph Analysis"
Author: T. Chen et al., 2020 – ACM Conference on Blockchain
This paper analyzes Ethereum scam activities by constructing transaction graphs and identifying behavioral patterns among fraudulent accounts. The authors demonstrate that graph-based methods can successfully detect scam clusters and identify links between malicious wallets.

3. "Graph Neural Networks for Cryptocurrency Transaction Classification"
Author: Y. Zhang et al., 2021 – IEEE Transactions on Neural Networks and Learning Systems
This research applies Graph Neural Networks (GNNs) to model wallet-to-wallet relationships and classify suspicious nodes in transaction graphs. The GNN-based model outperformed traditional machine learning approaches by capturing deeper transaction dependencies.

4. "Blockchain Analytics and Visualization for Forensic Investigation"
Author: M. R. Ali et al., 2022 – Elsevier Forensic Science International: Digital Investigation
The authors propose a blockchain forensic analysis system integrating visualization techniques to trace and interpret fund flow patterns. The system helps law enforcement visualize transaction chains and uncover hidden relationships among illicit wallets.

5. "Cross-Chain Cryptocurrency Analysis Using AI-Based Anomaly Detection"
Author: J. K. Sharma et al., 2023 – Springer Journal of Information Security and Applications
This recent work introduces an AI-driven framework capable of detecting anomalies across multiple blockchain networks. The system uses clustering and anomaly detection models to identify cross- chain laundering activities, improving overall tracing efficiency and transparency.

III. PROBLEM STATEMENT

The increasing adoption of cryptocurrencies has introduced new challenges in financial security and regulatory monitoring. While blockchain technology ensures transparency through public ledgers, its pseudonymous nature enables malicious users to conduct illicit activities such as money laundering, fraud, ransomware payments, and cross-chain fund transfers without revealing their real identities.

Existing blockchain explorers and forensic tools provide limited support for automated tracing and are typically restricted to single-chain analysis. They require manual wallet investigation, lack artificial intelligence capabilities, and do not offer real-time behavioral insights. Additionally, traditional databases used in these systems cannot effectively represent or analyze the complex network of wallet interactions that occur across multiple blockchains.

As a result, investigators and financial authorities face difficulties in:
- Identifying hidden wallet connections used for laundering or theft.
- Detecting cross-chain movements of illicit funds.
- Visualizing and interpreting transaction patterns effectively.

Hence, there is a pressing need for an AI-powered, multi-blockchain tracing system that can intelligently analyze wallet behaviors, detect anomalies, and represent fund flows using graph-based visualization. Such a system must integrate multiple blockchain APIs, apply machine learning and anomaly detection algorithms, and utilize a graph database (Neo4j) to uncover hidden relationships between wallets thereby enabling efficient and transparent investigation of suspicious cryptocurrency transactions.

IV. OBJECTIVES

The primary objectives are to:
1. To design and develop an AI-based framework capable of tracing and analyzing suspicious cryptocurrency transactions across multiple blockchain networks such as Ethereum and Binance Smart Chain.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411042|

2. To apply machine learning and anomaly detection techniques for identifying abnormal transaction behaviors and fraudulent wallet activities, including chain-hopping, tumbling, and fund layering.
3. To implement a graph-based data model using Neo4j that represents wallets and transactions as interconnected nodes and edges, enabling efficient relationship discovery and visual analysis of fund flows.
4. To create an interactive visualization and reporting interface that allows investigators and researchers to explore transaction graphs, detect suspicious patterns, and generate insights for forensic and regulatory purposes.

V. PROPOSED SYSTEM

The proposed system, "AI-Based Tracing of Suspicious Cryptocurrency Transactions Across Multiple Blockchains," is designed to enhance the detection and analysis of illicit activities occurring within cryptocurrency ecosystems. The architecture integrates blockchain data collection, AI-based transaction analysis, graph representation (Neo4j), and visual reporting to create an automated and intelligent tracing framework. Each component in the system contributes to identifying, analyzing, and visualizing suspicious patterns across multiple blockchain networks.

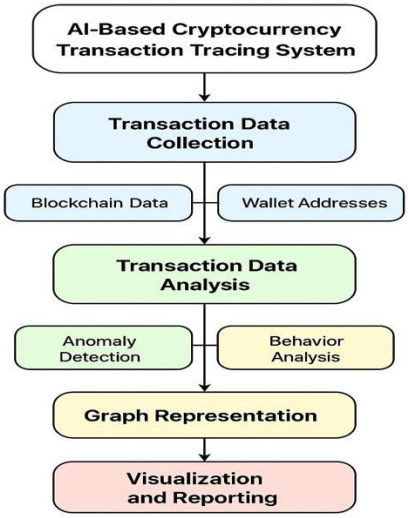


Fig.1: Proposed System Architecture

The process begins with the collection of blockchain transaction data from multiple sources using APIs such as Bitquery and Etherscan. These APIs allow the extraction of details including wallet addresses, transaction hashes, timestamps, and token values from various blockchain networks like Ethereum and Binance Smart Chain. By aggregating data from multiple blockchains, the system ensures a unified and comprehensive dataset for further analysis.

Once the data is collected, it undergoes preprocessing and analysis. During this stage, the system cleans and structures the data, removes redundancies, and organizes it into a machine-learning-compatible format. Artificial intelligence algorithms are then applied to detect abnormal transaction behaviors and identify suspicious wallets. The AI models analyze patterns such as direct transfers, distributed transfers, transfer-and-return cycles, and mixing or tumbling activities, which are commonly associated with laundering or fraudulent transactions. Through continuous pattern learning, the system can distinguish between normal and suspicious activities with higher accuracy.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411042|

VI. EXISTING SYSTEM

The existing blockchain tracing and analysis systems primarily rely on manual transaction tracking and single-chain monitoring tools such as Etherscan, Blockchain Explorer, and commercial platforms like Chainalysis and CipherTrace. These tools allow users to view wallet information, transaction history, and token transfers within a single blockchain network. However, they provide limited intelligence and lack the ability to analyze transactions that move across multiple blockchain ecosystems.

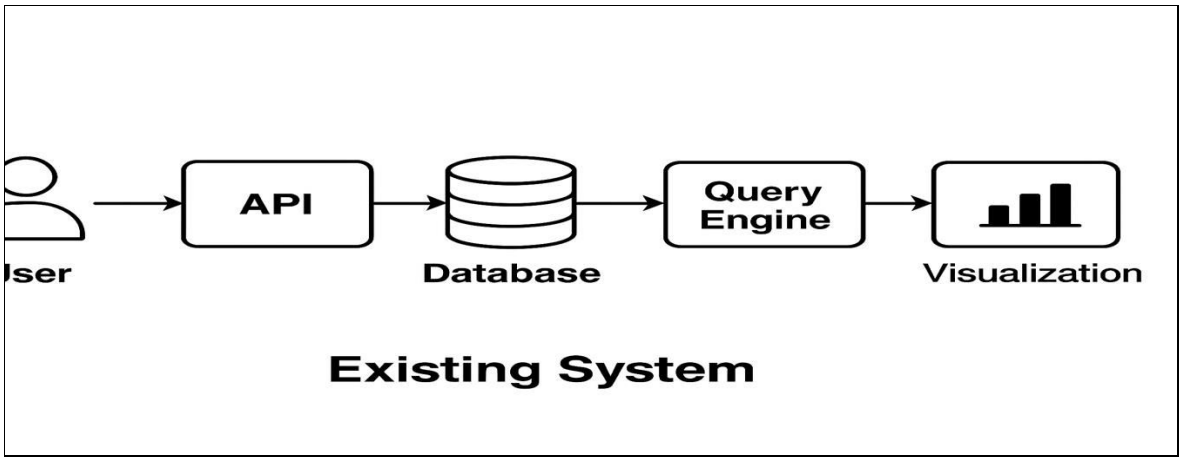


Fig.2: Existing System Architecture

VII. CONCLUSION & FUTURE WORK

This paper presents an approach for tracking addresses and transactions on the system. It assists in understanding the flow of funds and the behaviors of the thieves. By inputting the wallet addresses, we can examine transactions associated with those wallet addresses, including the amount of ETH transferred and all related transactions. This analysis aims to understand the money flow among different addresses by tracking the movements of ETH and ERC-20 tokens, especially the wallets contacting a centralized exchange that required KYC processes. The contribution of this work is to gather data from the blockchain analysis tool and examine thief behavior patterns using real thieves' wallet addresses. Eventually, we can identify suspicious transactions and behavioral patterns. This analysis can help us track the thief's identity. In addition, notification features will be implemented to detect anomaly patterns automatically in future work.

REFERENCES

1. **S. Weber, M. Baker, and C. Lin**, "A Machine Learning Approach for Detecting Illicit Cryptocurrency Transactions," IEEE Access, vol. 7, pp. 56345–56356, 2019.
2. **T. Chen, Y. Zhu, Z. Li, and X. Chen**, "Characterizing Ethereum Scams Using Transaction Graph Analysis," in Proceedings of the ACM Conference on Blockchain, Cryptocurrencies and Contracts (BChain), pp. 23–30, 2020.
3. **Y. Zhang and K. Wang**, "Graph Neural Networks for Cryptocurrency Transaction Classification," IEEE Transactions on Neural Networks and Learning Systems, vol. 32, no. 9, pp. 4185–4195, 2021.
4. **M. R. Ali, P. Johnson, and R. Gupta**, "Blockchain Analytics and Visualization for Forensic Investigation," Forensic Science International: Digital Investigation (Elsevier), vol. 40, 2022.
5. **J. K. Sharma and A. Bansal**, "Cross-Chain Cryptocurrency Analysis Using AI-Based Anomaly Detection," Journal of Information Security and Applications (Springer), vol. 70, 2023.
6. **Bitquery.io**, "Blockchain Data APIs for Analytics and Tracing," (Accessed 2024).
7. **S. Nakamoto**, "Bitcoin: A Peer-to-Peer Electronic Cash System," White Paper, 2008.
8. **Garcia, E., et al.** Hacker's Behavior Analysis: Insights from Blockchain Transactions. International Journal of Information Security, 32(4), 345-362. 2020

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411042|

9. **Lee, C., & Clark, M.** Examining the Holding Period of Stolen Funds: Insights from Hacker's Transactions. Journal of Digital Forensics, Security, and Law, 7(3), 89-105.2021

10. **Ansah, A.K.K., Adu-Gyamfi, D**. "Enhancing User and Transaction Privacy in Bitcoin with Unlinkable Coin Mixing Scheme." International Journal of Computational Science and Engineering, 23(4), 381-395. Inderscience Publishers.2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details