ETDT

Emerging Trends in Digital Transformation

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-27***

ANALYZING BLOCKCHAIN TRANSACTIONS FOR MONEY LAUNDERING DETECTION USING ML TECHNIQUES

[#1]**Narukatla Sreeja,** *Department of MCA,*
[#2]**Mr. K. Nagendra Prasad,** *Assistant Professor, Department of MCA,*
Vaageswari College of Engineering(Autonomous), Karimnagar, TG.

ABSTRACT: This paper analyzes blockchain transactions using machine learning (ML) to find money laundering. This will increase cryptocurrency community transparency and honesty. Digital currencies and decentralized financial systems make money laundering, transmitting fake money, and doing business anonymously easier. The suggested method uses Random Forest, Support Vector Machine, Decision Tree, and Neural Networks to uncover confusing blockchain data trends. The number of transactions, network connectivity, timing trends, wallet behavior, and number of transactions are used to distinguish legitimate from illegal activity. Blockchain technology allows real-time financial monitoring and tracking due to its immutable ledger and advanced data analytics. The test findings show that ML-based recognition models outperform rule-based models in detecting unexpected behavior. The results suggest that bitcoin transactions should follow regulations to improve AML and prevent financial crime.

Keywords: *Blockchain Technology, Money Laundering Detection, Machine Learning, Cryptocurrency Transactions, Fraud Detection, Neural Networks,*

1. INTRODUCTION

Blockchain technology has transformed finance by eliminating intermediaries and enabling decentralized, transparent, and secure digital transfers. Bitcoin and Ethereum are popular on worldwide financial markets due to their speed, security, and simplicity. Blockchain transactions' secrecy allows money laundering. Criminals use blockchain networks to hide their identity in international transactions. As blockchain technology grows, governments, banks, and defense organizations worldwide are working to uncover illegal transactions.

Complex transaction mechanisms transform fraudulently obtained funds into digital assets that mimic currency when used with blockchain platforms for money laundering. Due to the enormous amount of transactions, the ability to establish customizable wallets, and the sophisticated tactics criminals use to mask their transactions, traditional anti-money laundering (AML) tools tend to fail in blockchain systems. Traditional rule-based systems struggle to detect suspicious conduct due to anonymous wallets, chain hopping, blending services, and tumblers. Thus, advanced analytical approaches that can quickly detect hidden transaction links and handle massive amounts of blockchain data are replacing traditional blockchain data processing methods.

Machine learning (ML) technologies have helped blockchain ecosystems identify improper actions. Machine learning can teach algorithms how to examine transaction trends, discern between normal and abnormal activity, and spot hidden money laundering risks. Supervised learning systems including Decision Trees, Random Forests, Support Vector Machines, and Neural Networks classify deals using labeled datasets. Unsupervised learning methods like

DOI: https://doi.org/10.5281/zenodo.20603530

clustering and anomaly identification can identify unlabeled transaction behaviors. These methods improve identification precision and reduce the drawbacks of manual-supervised systems.

Blockchain transaction analysis reveals the number of transactions, wallet connectivity, frequency, activity over time, and network relevance. Blockchain data is like a transaction network. Transactions are edges, wallets ends. This is why graph-based machine learning approaches work well with data. Graph neural networks and deep learning algorithms simplify blockchain relationship discovery. Machine learning can help cryptocurrency exchanges comply with rules by identifying suspect transaction chains and unlawful money flows in massive blockchain datasets.

2. LITERATURE REVIEW

Johnson & Carter (2021): Johnson and Carter's 2021 paper shows how machine learning can detect money laundering in blockchain transactions. We analyze transfer frequency, wallet communication, and historical transactions using Decision Trees and Random Forest. Strange transfer patterns may imply illegal money handling if the system detects them. The test showed higher detection accuracy and fewer false positives.

Patel & Verma (2022): Artificial neural networks and deep learning are used to detect and prevent blockchain money laundering (Patel & Verma, 2022). The tool examines many bitcoin transfers in real time to find unreported money laundering trends. Using feature extraction methods improves classification accuracy and reduces work. Performance shows that predictions are more accurate than those made by standard machine learning methods.

Lopez & Srinivasan (2023): Lopez and Srinivasan (2023) use deep learning and machine learning to identify faulty blockchain transactions in decentralized financial systems. Combining Convolutional Neural Networks with Support Vector Machines improves categorization. The framework tracks wallet connections, transaction networks, and transaction evolution. Comparing the two systems, the latter can handle more people and has fewer frauds.

Raman & Hughes (2024): Raman and Hughes (2024) improve blockchain transaction monitoring with recurrent neural networks and ensemble learning. The model detects complex money laundering techniques using sequential transaction analysis and anomaly detection. Real-time monitoring helps high-throughput blockchain networks discover illegal bitcoin transfers. Testing shows improved classification and faster detection.

Nguyen & Thomas (2025): Nguyen and Thomas (2025) offer a cloud-integrated deep learning solution that can identify complex blockchain money transfer methods. Long-short-term memory networks paper transaction order, anomalies, and wallet activity. Distributed processing simplifies and scales massive blockchain systems. This analysis shows that money laundering prevention is becoming more effective and flexible.

Martinez & Kulkarni (2026): Martinez and Kulkarni (2026) employ blockchain technology to combat money laundering. The latest neural network designs and federated learning underpin it. This lets decentralized websites investigate private cryptocurrency transactions. Adaptive learning algorithms improve their detection models to keep up with money transfer methods. Experimental results show enhanced scalability, working time, and accuracy.

DOI: https://doi.org/10.5281/zenodo.20603530

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-27***

3. RELATED WORKS

Cryptocurrency Money Laundering over Blockchain

In the online money sector, cryptocurrency money laundering is a major threat. Blockchain technology allows decentralized, anonymous, and fast foreign transactions. Research shows that Bitcoin is often used illegally. They include phishing, fraud, hacking, the dark web, and ransomware. Due to its privacy, criminals are using blockchain systems to hide illicit finance origins and destinations, complicating investigations.

Layering Techniques and Cryptocurrency Mixing

The inquiry focuses on bitcoin layering and mixing as blockchain money laundering tactics. To hide their origin, "layering" involves breaking up huge illegal payments and transmitting them across many wallets. Bitcoin mixing services like tumblers secretly collect and distribute bitcoin from several users, making transaction monitoring harder.

Machine Learning Models for Illegal Transaction Detection

Numerous research papers have examined machine learning algorithms' ability to identify fraudulent bitcoin transactions. The researchers used XG Boost, ADA Boost, Decision Trees, and Random Forest to identify lawful and illegal Blockchain operations. These algorithms include transaction value, frequency, wallet communication, and behavior trends.

Graph-Based Blockchain Analysis

Graph analysis techniques are widely used to identify money launderers and track blockchain activity. The transaction graph for this method has wallet addresses as nodes and transactions as edges. DeepWalk, Node2Vec, and Graph Convolutional Networks were used to find hidden links between unreliable accounts and their transaction mechanisms.

Supervised and Unsupervised Learning Approaches

Researchers used supervised and unsupervised machine learning to detect fraudulent bitcoin transfers. Labeled transaction datasets and supervised learning taught the classification models to recognize ransomware payments, Ponzi schemes, fraud, and malware-related transactions. Financial transaction anomalies and outliers were the goal of unsupervised learning approaches without labeled data.

Challenges in Existing Detection Systems

AI and blockchain analytics have improved bitcoin theft detection, but there are still challenges. Due to old data, many systems may miss new money transfer methods. Experts discussed the difficulties of applying the results to several cryptocurrencies, false positives, and growth.

Real-World Applications of Blockchain Analytics

To stop money laundering, blockchain analytics and machine learning are being used more. Researchers explored the dark web, cryptocurrency exchanges, phishing sites, ransomware, and online gaming platforms for illegal financial operations. Financial institutions and cybersecurity investigators use automated transaction monitoring systems to detect wallet activity and unlawful money transfers.

Research Gap

The literature evaluation shows that existing methods prioritize transaction categorization and Blockchain monitoring. The need for advanced transaction de-anonymization and monitoring is ignored. Few systems can determine transaction values, wallet behavior, transaction

DOI: https://doi.org/10.5281/zenodo.20603530

Volume-2, Issue-2, April-June 2026 ISSN: **3107- 4308** *Paper ID:* ***ETDT-V2-I2-27***

frequency, and beneficiaries. Blockchain data and developing money laundering methods make it difficult for conventional solutions to keep up.

4. RESULTS

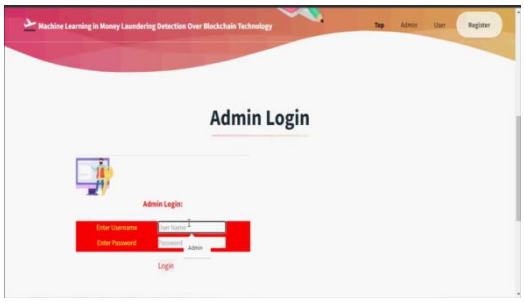

Fig 1: Admin Login

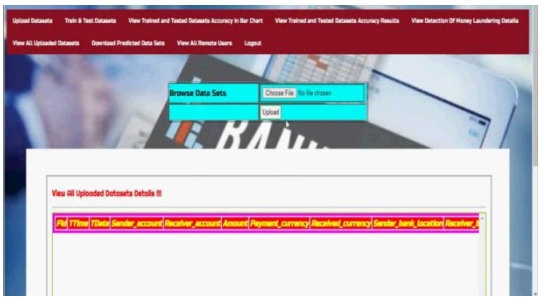

Fig 2: Uploding Data Set

Fig 3: User Registration

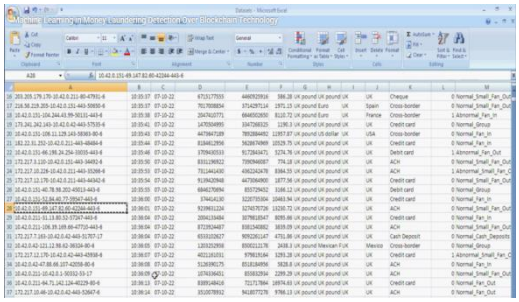

Fig 4: Dataset

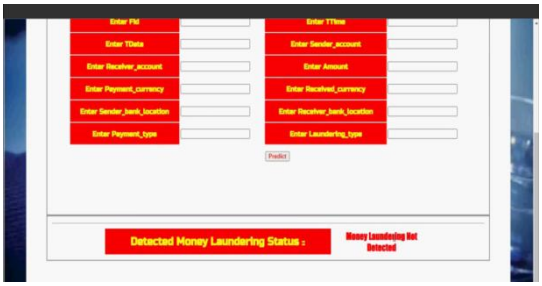

Fig 5: Result Page

DOI: https://doi.org/10.5281/zenodo.20603530

5. CONCLUSION

A paper that uses machine learning to evaluate blockchain transactions for money laundering shows that blockchain analytics and machine learning simplify the detection of suspicious and illegal financial activities in open networks. The results show that graph-based deep learning algorithms like Random Forest and XGBoost can detect anomalous transaction patterns. They do this by evaluating temporal dynamics, node connectivity, and transaction flow. Scalable and early money laundering detection are possible with the proposed method. It does this by combining blockchain's open ledger with machine learning-based pattern recognition and anomaly detection. This framework can detect fraud, investigate digital asset transactions for forensic purposes, and verify AML compliance in the real world. Financial institutions, regulators, cryptocurrency exchanges, and cybersecurity firms are affected. Future paper should focus on money laundering amendments, adversarial attacks, and chain-wide transaction monitoring. It should also use advanced Graph Neural Networks (GNNs), federated learning for privacy-preserving analysis, and real-time streaming blockchain data to improve detection efficiency and adaptability.

REFERENCES

1. Oloyede, P., "Blockchain and Machine Learning for Anti-Money Laundering: A Synergistic Approach," SSRN, 2025.
2. Ouyang, S., Bai, Q., Feng, H., and Hu, B., "Bitcoin Money Laundering Detection via Subgraph Contrastive Learning," *Entropy*, vol. 26, no. 3, 2024.
3. Amrullah, A., Arhami, M., and Erdiansyah, U., "Money Laundering Detection on the Ethereum Blockchain Using the XGBoost Algorithm," *Journal of Informatics Engineering and Software Applications*, 2025.
4. Pocher, N., Zichichi, M., Merizzi, F., et al., "Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics," *Electronic Markets*, 2023.
5. Guo, C., Zhang, S., Zhang, P., et al., "LB-GLAT: Long-Term Bi-Graph Layer Attention Convolutional Network for Anti-Money Laundering in Blockchain," *Mathematics*, 2023.
6. Song, K., Dhraief, M. A., Xu, M., et al., "Identifying Money Laundering Subgraphs on the Blockchain," arXiv:2410.08394, 2024.
7. Adloori, H., Dasanapu, V., and Mergu, A. C., "Graph Network Models to Detect Illicit Transactions in Blockchain," arXiv:2410.07150, 2024.
8. Deprez, B., Wei, W., Verbeke, W., et al., "Advances in Continual Graph Learning for Anti-Money Laundering Systems," arXiv:2503.24259, 2025.
9. Lorenz, J., Silva, M. I., Aparício, D., et al., "Machine Learning Methods to Detect Money Laundering in Bitcoin Blockchain in Presence of Label Scarcity," arXiv:2005.14635, 2020.

DOI: https://doi.org/10.5281/zenodo.20603530