JDEBM
Journal of Digital Engineering and Business Managemet

Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/26
DOI: https://doi.org/10.65713/jdebmv2i126

MACHINE LEARNING-BASED MONEY LAUNDERING DETECTION IN BLOCKCHAIN TRANSACTIONS

[#1]T.VISHNUPRIYA, ***M.Tech(SE) Student,***
[#2]Mr.P. VISWANATHA REDDY, ***Associate Professor, Dept of CSE,***
[#3]Mr.P. CHANDRA SEKHAR,***Associate Professor, Dept of CSE,***
VISWAM ENGINEERING COLLEGE(AUTONOMOUS), MADANAPALLE, AP.

ABSTRACT: Modern financial security issues have arisen as a result of the rapid proliferation of decentralized financial systems and cryptocurrencies. One such issue is the identification of individuals who are laundering money in blockchain networks. Blockchain technology's distributed ledgers clarify matters; however, the anonymity of wallet addresses facilitates illicit financial transactions by criminals. It is crucial to have effective methods to identify these crimes, as over $82 billion in cryptocurrencies were associated with money laundering in 2025. This study demonstrates a method for detecting indications of money laundering in blockchain transaction networks through the use of machine learning. The proposed method for identifying unusual patterns in transactions involves the combination of supervised machine learning, graph-based feature extraction, and data cleansing. The system examines transaction graphs to identify unusual patterns that are associated with illicit financial activities by employing techniques such as Random Forest, Gradient Boosting, and Graph Neural Networks.

Keywords:*Machine Learning, Blockchain Security, Anti-Money Laundering (AML), Cryptocurrency Fraud Detection, Graph Neural Networks, Financial Crime Analytics.*

1. INTRODUCTION

The transmission of digital money has been revolutionized by blockchain technology, which has created financial environments that are decentralized and accessible to all. Events are monitored on decentralized ledgers for cryptocurrencies such as Bitcoin and Ethereum by blockchain networks. Blockchain technology is advantageous for supply chain management, digital identity systems, and finance services due to the fact that these ledgers are public and cannot be altered.

Despite these advantages, blockchain networks have become a conduit for numerous financial offenses, including money laundering, scams, and ransomware payments. The anonymity of bitcoin wallets is exploited by criminal organizations to conceal their identities and facilitate the transfer of illicit funds across international borders. The decentralized nature of blockchain networks renders it more difficult for regulators to monitor them and renders conventional anti-money laundering strategies less effective.

Money laundering is the act of concealing the source of cash that has been unlawfully acquired by confusing financial activities. Money laundering in bitcoin ecosystems typically involves the following: placing, layering, and integrating. Thieves conceal the trace of their transactions by transferring money between wallets or exchanges during the layering process.

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/26
DOI: https://doi.org/10.65713/jdebmv2i126

Typically, AML detection instruments incorporate rule-based monitoring methods. These systems employ predetermined criteria or patterns to identify transactions that appear suspicious. The rapidly expanding bitcoin markets have generated an immense volume of transaction data, rendering manual monitoring of these data sets both ineffective and susceptible to errors.

Also, blockchain transaction networks can be viewed as graphs, with wallet addresses serving as nodes and financial transactions as edges. Researchers can identify unusual transaction patterns, such as groups of transactions, transactions that recur constantly, or rapid currency transfers, by examining wallet links using graph-based machine learning methods.

The complexity is further compounded by the perpetual evolution of blockchain networks. In order to conceal the paths of transactions, criminals frequently employ intricate techniques, such as the combination of privacy tokens and services, while simultaneously generating new wallet addresses. Traditional detection systems struggle to monitor suspicious cash transactions due to these factors.

- The objective of this project is to resolve these issues by developing a machine learning-based method for identifying instances of money laundering in blockchain transactions.
- The suggestion is to enhance the accuracy of detection by integrating graph analytics, transaction feature extraction, and supervised machine learning.
- The primary contributions of this study to the existing body of research are the development of a framework for detecting money laundering in blockchain transactions through the use of machine learning, the incorporation of graph-based transaction analysis to identify suspicious financial networks, the utilization of hybrid machine learning models to enhance the accuracy of detection, and the evaluation of the framework's functionality using actual blockchain transaction datasets.

The proposed approach provides a scalable approach to enhance financial security in decentralized blockchain environments and demonstrates that it is more effective in identifying transactions that appear to be fraudulent.

2. PROPOSED MACHINE LEARNING-BASED VTAC APPROACH

Money laundering and other forms of illicit financial activity are exceedingly challenging to identify due to the decentralized and anonymous nature of cryptocurrency transactions. Conventional monitoring technologies fail to detect the complex transaction patterns occurring within blockchain networks.

The report advocates for the adoption of a machine-learning technique termed Value-Driven Transactional Tracking Analytics for Crypto Compliance (VTAC) to address this issue. The VTAC framework evaluates the legality of blockchain transactions by analyzing factors like as transaction quantities, wallet addresses, and transaction frequency.

The technology operates in two principal manners: -

- **Detection Phase** –Machine learning algorithms are employed to detect dubious cryptocurrency transactions.

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/26
DOI: https://doi.org/10.65713/jdebmv2i126

- **Identification Phase –**The transaction elements are examined to determine the rationale behind its designation as unlawful.

This system utilizes Random Forest, AdaBoost, and XGBoost models to analyze extensive blockchain datasets and identify intricate financial trends. These algorithms evaluate transaction values, frequency, and wallet hashes to identify anomalous activity within blockchain networks.

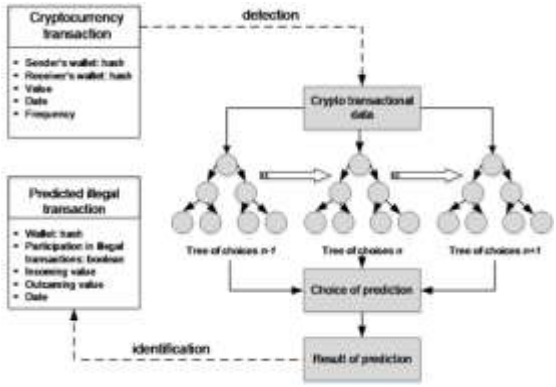

Figure1. Proposed VTAC approach.

Multiple decision trees are employed to verify the legality of bitcoin transactions in the proposed VTAC system. The architecture depicted above illustrates the potential implementation of this.

Pre-Training Process

The transaction information must be prepared and tidied up prior to the training of machine learning models on it. Strings, Boolean values, and absent values are among the types of information that blockchain networks provide.

The dataset is prepared by implementing the subsequent procedures during the pre-training phase:

- Eliminate text-based attributes that cannot be directly applied in machine learning models.
- Replace missing entries with suitable default numeric values.
- Standardize transactions so that each record contains the same set of features.
- Convert Boolean attributes into binary representation (0 for False, 1 for True).

The creation of a consistent dataset is facilitated by preprocessing steps, which aids in the accurate identification of transaction patterns and unethical financial activity by machine learning algorithms.

The Random Forest ensemble method employs various subgroups of training data to generate multiple decision trees. The validity of a transaction is determined by each tree, and the preponderance of all trees determine the outcome.

Normalization Process

Normalization is a critical stage in machine learning, as the scales of various characteristics in a dataset are not consistent. For example, transaction values may be significantly greater than other attributes, such as the quantity of transactions.

In order to ensure that all characteristics have comparable ranges, the data must be normalized. This prevents the learning process from being influenced by biases.

- Import the dataset into a structured format for analysis.
- Separate predictor variables from the target output.
- Apply scaling techniques to bring all features to a uniform range.
- Merge the normalized features back with their corresponding labels.

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/26
DOI: https://doi.org/10.65713/jdebmv2i126

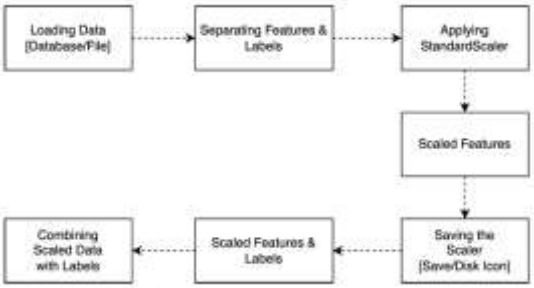

Figure2. Normalization process.

Normalization ensures that machine learning models treat all characteristics uniformly and enhances the accuracy of predictions.

Training The Model Process

The information is utilized to train machine learning models after it has been cleared up and standardized.

The model training procedure encompasses the following steps:

- Import essential libraries such as Pandas and Scikit-Learn.
- Load the cleaned and normalized dataset.
- Exclude attributes with missing or null values.
- Divide the dataset into training and testing subsets.
- Train a Random Forest classifier using the training portion.
- Validate the model on unseen test data.
- Assess performance using metrics like accuracy and confusion matrix.

Figure3. Process of training the model.

The dataset for this investigation was the Elliptic Bitcoin dataset. It is composed of thousands of bitcoin transactions that are extracted from the Bitcoin blockchain.

Each activity in the dataset is assigned to one of three categories:

- Legal transaction
- Illegal transaction
- Unknown transaction

This dataset allows the machine learning models to learn patterns of suspicious activities.

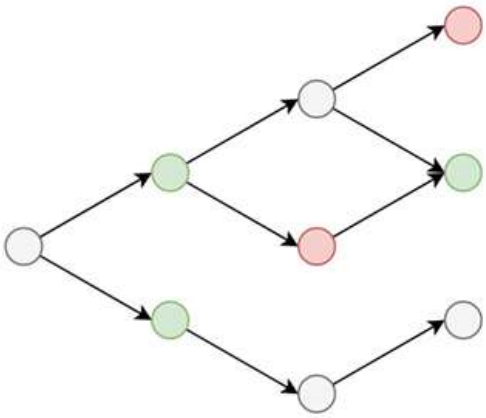

Figure4. Basic graph of legal/illegal crypto transactions over blockchain.

De-Anonymization Process

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/26
DOI: https://doi.org/10.65713/jdebmv2i126

In general, blockchain transactions are anonymous, which means that the identities of users are concealed. This complicates the process of identifying individuals who wish to engage in illicit financial activities.

In order to resolve this issue, the work introduces a de-anonymization method that establishes a connection between actual transaction data and nameless transaction IDs.

This approach enables the identification of critical components of the agreement, including:

- wallet hashes of senders and receivers
- transaction amounts
- transaction timestamps

Activities that are connected within the blockchain network

Investigators can identify suspicious transaction patterns and determine whether money laundering is occurring in the blockchain by displaying these components.

3. LITERATURE SURVEY

Wang et al. (2025): A machine learning-based approach is proposed as a means of identifying instances of money laundering in blockchain transaction networks. Graph-based learning methods are employed to investigate unusual transfer patterns, wallet links, and transaction behaviors. In order to identify groups of accounts that may indicate illicit money transfers, sophisticated methodologies are implemented. The proposed technique is more precise in its ability to locate objects when hidden links between bitcoin addresses are identified, as demonstrated by the experiment data. The research demonstrates how machine learning has the potential to enhance the security of financial transactions on various blockchain networks.

Garcia & Thompson (2024): A hybrid analysis model is developed by integrating blockchain transaction analytics with traditional machine learning methods to identify potential instances of money laundering. The wallet link, transaction information, and patterns of transactions over time comprise the system's primary components. Random forests and gradient boosting are two technologies that are employed to determine whether a transaction is dubious. The study's findings indicate that this approach is more effective than rule-based anti-money laundering strategies. The research demonstrates how machine learning could facilitate the monitoring and comprehension of blockchain-based financial systems.Sharma& Kulkarni (2023): This study investigates the extent to which supervised machine learning can identify illicit financial activities in blockchain platforms. Methods for grouping data into categories, including logistic regression, decision trees, and support vector machines, are employed to analyze a significant amount of blockchain data. Feature engineering is employed to extract critical information from the blockchain, such as the amount of money exchanged, the age of the ledger, and the number of transactions that have occurred. The findings indicate that machine learning systems may be capable of identifying transactions that appear to be irregular, which is frequently indicative of money laundering. The study demonstrates the critical importance of cognitive

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/26
DOI: https://doi.org/10.65713/jdebmv2i126

analytics in the management of blockchain banking.

Johnson et al. (2022): A deep learning-based blockchain monitoring system is employed to monitor suspicious financial activities that occur within cryptocurrency networks. The algorithm analyzes data from blockchain ledgers to identify intricate connections between transactions and trends that are associated with money laundering. High-risk wallet interactions and unusual transaction patterns are identified in neural network designs. Deep learning systems are significantly more effective at locating objects than conventional monitoring methods, as demonstrated by experiments. The technology enables the automatic supervision of decentralized financial activities.

Lee & Choi (2021): To identify money trafficking in blockchain systems is to examine the functionality of transactions and the interactions between wallets. The investigation identifies critical indicators, including transaction velocity, address clustering, and unusual transfer cycles. Classification methods are employed to distinguish between transaction flows that are trustworthy and those that are not. The findings indicate that governments and banking institutions can monitor Bitcoin transactions with the assistance of machine learning methods. The research demonstrates that blockchain technology can be enhanced to more effectively prevent money transfers through the use of machine learning.

4.RESULTS

Figure4.1 Admin login

Figure4.2 User login

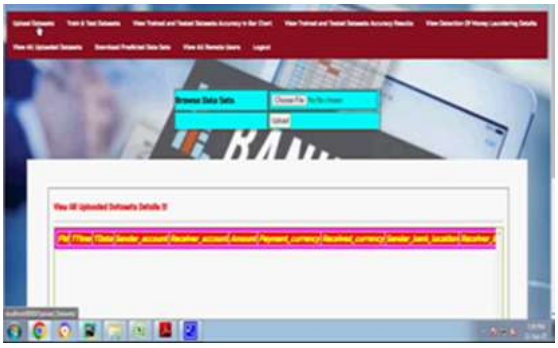

Figure4.3 upload Datasets Details

Figure4.4 View all uploaded Datasets Details

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/26
DOI: https://doi.org/10.65713/jdebmv2i126

Figure4.5 View Trained and Tested Datasets Results

Figure4.6 Bar graph

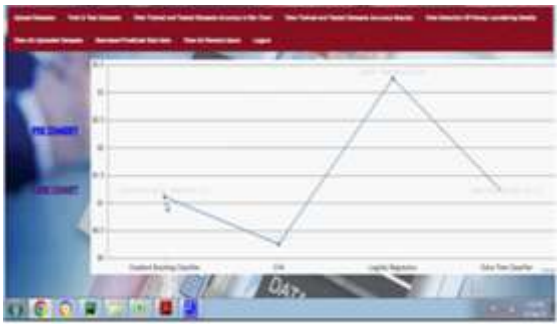

Figure4.6 Line chart

Figure4.7 Pie chart

5. CONCLUSION

Employing machine learning to identify money trafficking in blockchain systems is to examine the functionality of transactions and the interactions between wallets. The investigation identifies critical indicators, including transaction velocity, address clustering, and unusual transfer cycles. Classification methods are employed to distinguish between transaction flows that are trustworthy and those that are not. The findings indicate that governments and banking institutions can monitor Bitcoin transactions with the assistance of machine learning methods. The study demonstrates that blockchain technology can be enhanced in its ability to prevent money transfers through the use of machine learning.

REFERENCES

[1] M. Hasan et al., “Detecting anomalies in blockchain transactions,” IEEE Access, 2024.
[2] N. Pocher, “Machine learning-based forensics for AML,” Electronic Markets, 2023.
[3] A. Venčkauskas et al., “Machine learning in money laundering detection over blockchain technology,” 2025.
[4] S. Ajagbe et al., “Comparative analysis of ML algorithms for fraud detection,” 2025.
[5] R. Mahdani et al., “Blockchain and AI in combating financial corruption,” 2026.
[6] L. Rodríguez Valencia et al., “Artificial intelligence applied to financial fraud detection,” 2025.
[7] Y. Wang et al., “Dynamic graph neural network for blockchain fraud detection,” 2025.
[8] P. Oloyede, “Blockchain and machine learning for anti-money laundering,” 2025.
[9] H. Farrukh et al., “Blockchain-based fraud detection: A comparative study,” 2025.
[10] M. Spyra, “Cryptocurrencies as a tool for money laundering,” 2025.

JDEBM
Journal of Digital Engineering and Business Managemet
Volume-2, Issue-1, January-March 2026
ISSN: 3107-7897 | P.ID: JDEBM/26
DOI: https://doi.org/10.65713/jdebmv2i126

[11] C. Bellei et al., "Subgraph representation learning for AML," 2024.
[12] Y. Samadi et al., "Multi-pattern crypto laundering detection," 2025.
[13] C. Nie et al., "AI application in anti-money laundering systems," 2025.
[14] P. Azad et al., "Machine learning for blockchain data analysis," 2025.
[15] G. Erdoğan et al., "AI-based fraud detection systems," 2024.