International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 1, 2026

Peer Reviewed, Referred & Indexed Journal

Research

Detection of Illicit Cryptocurrency Transactions Using Hybrid XGBOOST–Random Forest and LIGHTGBM Models

Dr.M.CHAITANYA KISHORE REDDY1, RAMINENI NEELIMA2, PAGOLU SUJITH KUMAR3, VATAPALLI NIKILESH BABU4

#1 Professor of the Information Technology Department,NRI Institute Of Technology,Agiripalli

#2#3#4 B.Tech with Specialization of Information Technology in NRI Institute Of Technology,Agiripalli

Abstract: Because blockchain networks are decentralized and pseudonymous, money laundering through bitcoin transactions has become a major concern. When dealing with big and complicated transaction datasets, traditional machine learning techniques for unlawful transaction identification frequently have poor generalization and limited accuracy. This paper suggests an improved money laundering detection system that makes use of hybrid machine learning and sophisticated boosting techniques in order to overcome these constraints. By incorporating a hybrid model that combines XGBOOST and Random Forest with potent boosting algorithms like LIGHTGBM and CATBOOST, the system improves detection capabilities above current methods. To find high-frequency and multilayer transaction patterns frequently linked to money laundering operations, Value-driven Transactional Analytics for Crypto Compliance (VTAC) is used. The suggested method greatly enhances predictive performance, as demonstrated by experimental assessment on the Elliptic Bitcoin Dataset, where LIGHTGBM achieved the maximum accuracy of 99.85%. The findings demonstrate that hybrid and advanced boosting models offer better accuracy, scalability, and resilience, which makes the suggested framework ideal for real-time blockchain compliance and anti-money laundering applications.

Index terms - *Money Laundering Detection, Blockchain Technology, Cryptocurrency Transactions, Machine Learning, Hybrid Models, Boosting Algorithms, LIGHTGBM, VTAC, Crypto Compliance, Illicit Transaction Detection*

Received: 17-01-2026 Accepted: 20-02-2026 Published: 28-02-2026

1. INTRODUCTION

Due to the decentralized, transparent, and peer-to-peer transactions made possible by the explosive rise of blockchain technology and cryptocurrencies, digital financial institutions have undergone substantial change. Although these features improve efficiency and security, they have also raised

significant security issues. Cryptocurrency abuse for illicit purposes including money laundering, drug trafficking, ransomware payments, arms selling, and the sale of stolen personal information has increased with the rise of the dark web. A significant danger to global financial security, cryptocurrencies have emerged as a favored means for cybercriminals to transfer illegal payments anonymously due to the lack of centralized management and regulatory supervision [1].

Because of its popularity, liquidity, and widespread acceptability, Bitcoin has been frequently used for illicit financial transactions among other cryptocurrencies. Numerous studies have shown that a sizable percentage of bitcoin transactions are connected to illegal activity, underscoring the pressing need for efficient detection systems [2]. The pseudonymous nature of wallet addresses makes it challenging to directly link transactions with real-world identities, even when blockchain transactions are publicly published. Traditional Anti-Money Laundering (AML) enforcement is made more difficult by this restriction, which enables criminals to conceal money flows through the use of strategies like transaction chaining, mixing services, and tumblers.

The problem of money laundering has been made worse in recent years by the rise in phishing assaults, cryptocurrency breaches, and exploit-based crimes. Cybercriminals frequently take advantage of weaknesses in wallets, smart contracts, and exchanges to steal digital assets, which are subsequently laundered via intricate transaction patterns across several platforms and addresses [3]. Crypto-related attacks have reportedly cost billions of dollars, underscoring the increasing complexity of illegal financial activities in blockchain ecosystems [4]. Intelligent and flexible detection systems that can recognize suspicious activity beyond basic rule-based monitoring are necessary in light of these changing assault tactics.

Blockchain technology has both advantages and disadvantages when it comes to financial security, despite its creative design. The absence of built-in identity verification systems and regulatory enforcement is a significant disadvantage for crime prevention, even though transparency and immutability are significant benefits [5]. The majority of current AML systems are based on conventional machine learning or graph-based techniques, which frequently have issues with scalability, unbalanced data, and changing laundering tactics. In order to properly capture high-frequency and multilayer transaction patterns, these systems usually concentrate on traditional transaction attributes and lack sophisticated modeling approaches.

By combining sophisticated boosting and hybrid machine learning algorithms, this work suggests an improved money laundering detection framework that goes beyond current methods in order to get over these drawbacks. The suggested method increases prediction accuracy, scalability, and resilience by fusing cutting-edge boosting algorithms like LIGHTGBM with potent ensemble models like XGBOOST–Random Forest hybrids. In order to better identify sophisticated laundering operations, Value-driven Transactional Analytics for Crypto Compliance (VTAC) is also integrated to examine transaction value and frequency trends. A scalable and high-performing solution for blockchain-based

AML and crypto compliance monitoring is offered by this integrated method.

2. LITERATURE SURVEY

i) Zerocash: Decentralized Anonymous Payments from Bitcoin
https://ieeexplore.ieee.org/document/6956581

The first digital money to be widely used was BitCoin. Although Bit Coin facilitates payments between pseudonyms, it is unable to provide robust privacy assurances since payment transactions are documented in a publicly accessible decentralized ledger from which a great deal of information may be inferred. By separating transactions from the source of the payment, Zero Coin (Miers et al., IEEE S&P 2013) addresses some of these privacy concerns. However, its functionality is still restricted and it still displays the destinations and amounts of payments. We build a complete ledger-based digital currency with robust privacy protections in this article. Our findings take use of recent developments in Succinct Non-interactive Arguments of Knowledge (zk-SNARKs), which are zero-knowledge arguments. Decentralized anonymous payment systems (DAP schemes) are the first thing we design and build. By hiding the payment's origin, destination, and transmitted amount in the related transaction, a DAP scheme allows users to pay one other directly and secretly. We give explicit definitions and demonstrate the security of the architecture. Second, we develop Zero Cash, a real-world implementation of our DAP scheme design. Transactions in Zero Cash are less than 1 kB and take less than 6 ms to verify, making it comparable with ordinary Bit coin and orders of magnitude more efficient than the less anonymous Zero currency.

ii) Traceable Monero: Anonymous Cryptocurrency with Enhanced Accountability
https://ieeexplore.ieee.org/document/8685178

High levels of anonymity are offered by Monero for both users and transactions. However, the anonymity offered by bitcoin transactions may allow for the commission of several illegal acts. As a result, user responsibility, also known as traceability, is crucial in Monero transactions and is sadly absent from the literature at this time. In order to bridge this gap, we present Traceable Monero, a brand-new cryptocurrency that strikes a balance between user accountability and anonymity. Although our approach depends on a tracing authority, it is optimistic in that it only becomes engaged when it is necessary to conduct inquiries into specific transactions. We formalize Traceable Monero's security and system models. By overlaying Monero with two different tracing mechanisms—tracing the long-term addresses and the one-time addresses with money flows—we show a thorough architecture of Traceable Monero. We illustrate the security of Traceable Monero and put the system prototype into practice, showing that, in comparison to Monero transactions, Traceable Monero has only a very minor cost in transaction generation and verification.

iii) Detecting Roles of Money Laundering in Bitcoin Mixing Transactions: A Goal Modeling and Mining Framework
file:///C:/Users/hajar/AppData/Local/Temp/MicrosoftEdgeDownloads/df88c16d-0faa-4c13-943d-f91b73a53ba2/fphy-09-665399.pdf

Money laundering has found a new home in cryptocurrency. Bitcoin mixing services purposefully obscure the sender-receiver link, making it challenging to track down questionable financial transactions. We think that understanding the roles

that agents play in the money laundering process is essential to demythologizing bitcoin mixing services. Using historical bitcoin transaction data, we provide a goal-oriented method for modeling, identifying, and evaluating various role types in the agent-based business process of the bitcoin mixing scenario. It examines the roles in the bitcoin money laundering process from the standpoint of the agents' goals. Additionally, it offers a starting point for learning about the responsibilities played by actual agents in bitcoin money laundering situations.

iv) Regulating the Metaverse Economy: How to Prevent Money Laundering and the Financing of Terrorism
https://www.researchgate.net/publication/377040383_Regulating_the_Metaverse_Economy_How_to_Prevent_Money_Laundering_and_the_Financing_of_Terrorism

We help candidates remain watchful and make smart decisions by using machine learning (ML) to predict the possibility that a job is fake. This, in turn, decreases the amount of fake job ads on the internet. The model extracts features using the TF-IDF vectorizer and using natural language processing to analyze trends and attitudes in job postings. With the help of Random Forest and SMOTE, the balanced data will be accurately categorized. It prevents overfitting and improves model accuracy even with big datasets. The final algorithm will find out if the job is real or not by looking at the details of the listing.

v) Cryptocurrency tumbler: legality, legalization, criminalization
https://www.researchgate.net/publication/355161998_Cryptocurrency_tumbler_legality_legalization_criminalization

Tumbler is a cryptocurrency service that is offered when anonymity is at risk and it is possible to identify the owner of virtual "coins." Since not even bitcoin values are legal and "mixing" them in tumblers is a particular treatment of them, the legality of cryptocurrency tumblers might be characterized as a "grey zone." The author of this study examines and presents all of the unanswered concerns regarding cryptocurrency tumblers, including their legality, legalization, and most importantly, the possibility of future criminality, using analytical, descriptive, and comparative methods. The author's final conclusion is that legality, legalization, and criminalization are closely related and interconnected, and that lawmakers everywhere should exercise extreme caution when legalizing tumblers, particularly if they intend to criminalize them later.

3. METHODOLOGY

i) Proposed Work:

Through the use of sophisticated boosting and hybrid learning algorithms, the proposed project seeks to improve money laundering detection in blockchain-based cryptocurrency transactions. To extract valuable transactional data such wallet hash behavior, transaction value, temporal trends, and transaction frequency, the system makes use of Value-driven Transactional Analytics for Crypto Compliance (VTAC). To guarantee high-quality input data, these characteristics are handled via a systematic preprocessing pipeline that includes conventional normalization, numeric encoding, and handling of missing values. To provide a solid baseline for detection performance, machine learning models like as Random Forest, XGBOOST, and ADABOOST are

first used to categorize transactions as lawful or illicit.

The suggested method incorporates hybrid and advanced boosting models as a crucial addition to further enhance accuracy, scalability, and generalization. To capitalize on the advantages of both ensemble decision trees and gradient boosting, a hybrid model that combines XGBOOST and Random Forest is created. Furthermore, cutting-edge boosting algorithms like CATBOOST and LIGHTGBM are included to effectively manage intricate and sizable blockchain information. These models are intended to identify aberrant, multilayer, and high-frequency transaction patterns that are frequently linked to money laundering. The system provides a strong and useful foundation for real-time crypto compliance monitoring and anti-money laundering enforcement by producing projected illicit transactions together with related wallet hash addresses, transaction values, and timestamps.

ii) System Architecture:

An effective and scalable framework for identifying illegal bitcoin transactions on blockchain networks is provided by the system architecture. Raw bitcoin transaction data, such as sender and recipient wallet hash addresses, transaction value, date, and frequency, is first gathered. The detection layer receives this transactional data once it has been arranged as crypto transactional data. To provide consistent data representation, the preprocessing module resolves missing values, transforms non-numeric features into numerical form, and uses standard normalization. Reliable learning is made possible by this organized data preparation, which also lowers noise in later phases of analysis.

The machine learning and decision-making layer processes the transaction data after preprocessing, producing prediction results from a variety of ensemble and boosting-based models. This layer examines transactional behavior from many angles using sequential decision structures, which are represented as several trees of options. To find the most confident classification, the prediction selection module aggregates the outputs from models like Random Forest, XGBOOST, hybrid XGBOOST–Random Forest, LIGHTGBM, and CATBOOST. Along with the corresponding wallet hash addresses, incoming and outgoing values, and transaction dates, the final output module generates the prediction result, identifying illicit transactions. With this design, blockchain-based anti-money laundering and crypto compliance monitoring systems are guaranteed precise identification, effective scalability, and feasible implementation.

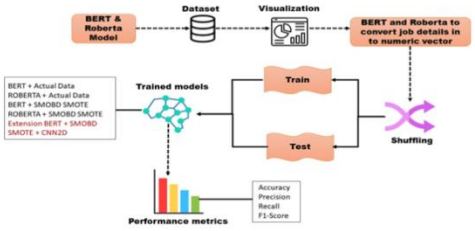

Fig.1. Proposed Architecture

iii) MODULES:

a) Transaction Data Collection Module

This module is in charge of gathering the blockchain dataset's raw bitcoin transaction facts. It collects key information such transaction value, transaction date, transaction frequency, sender wallet hash, and recipient wallet hash. The gathered information serves as the basis for additional investigation and identification.

b) Data Preprocessing Module

The gathered transaction data is cleaned and ready for machine learning by this module. It uses conventional scaling for normalization, manages missing values,

and transforms non-numeric data into numeric representations. Accuracy and dependability of the model are increased and consistent input is guaranteed by proper preprocessing.

c) VTAC Feature Analysis Module

Transaction values, frequency, and temporal trends are examined by the Value-driven Transactional Analytics for Crypto Compliance (VTAC) module. It detects irregular value movements and high-frequency transactions that point to money laundering activity. For efficient detection, this module improves feature representation.

d) Machine Learning and Hybrid Modeling Module

In addition to hybrid and sophisticated boosting models like XGBOOST–Random Forest, LIGHTGBM, and CATBOOST, this module applies machine learning methods like Random Forest, XGBOOST, and ADABOOST. Based on patterns it has learnt, it trains these models to categorize transactions as either lawful or illicit.

e) Prediction Selection Module

The results of several models and decision trees are combined by the prediction selection module. It chooses the most accurate categorization result after assessing each prediction's level of confidence. This ensemble-based decision-making process lowers false positives and increases resilience.

f) Result and Reporting Module

The final prediction results are shown in this module, which also identifies illicit transactions and the corresponding wallet hash addresses. It shows the values of incoming and departing transactions together with the dates that correspond to them. According to the findings, blockchain-based anti-money laundering and crypto compliance systems may be effectively monitored, investigated, and enforced.

iv) ALGORITHMS:

a) Random Forest

The ensemble learning method Random Forest creates several decision trees using random training data and feature sets. Each tree learns transaction behavior separately, and majority voting predicts. This method minimizes variance and overfitting in highly unbalanced bitcoin transaction datasets. Random Forest is a powerful baseline model in the proposed system, encapsulating value distribution, transaction counts, and wallet interaction patterns. This resilience makes it useful for first suspicious transaction identification.

b) XGBOOST

XGBOOST (Extreme Gradient Boosting) optimizes a differentiable loss function to build models consecutively. New trees correct past errors, allowing the model to learn complicated non-linear transaction data correlations. Structured transfers and repetitive low-value transactions are easily detected by XGBOOST in blockchain AML detection. Built-in regularization prevents overfitting and improves generalization. The method improves prediction accuracy in the suggested framework.

c) ADABOOST

The ensemble approach ADABOOST (Adaptive Boosting) dynamically alters training sample relevance dependent on classification difficulty. Early misclassified transactions are weighted more, prompting the algorithm to focus on infrequent and suspected laundering. This makes ADABOOST effective at spotting rare unlawful transactions. ADABOOST boosts illegal transaction recollection and anomaly detection in the proposed system.

d) Hybrid XGBOOST–Random Forest

Gradient boosting and bagging-based ensembles complement each other in the hybrid XGBOOST–Random Forest model. XGBOOST learns complex feature relationships and transaction dependencies, whereas Random Forest is stable and noise-resistant. The hybrid strategy balances bias and variance by combining both models' predictions. This hybrid model detects complicated laundering methods including layering and fast fund circulation, a major improvement above standard AML models.

e) LIGHTGBM

Advanced gradient boosting framework LIGHTGBM is efficient and scalable on huge datasets. Leaf-wise tree growth and histogram-based splitting improve training time without compromising accuracy. LIGHTGBM supports high-dimensional transaction attributes and big data sets in blockchain analytics. LIGHTGBM is the best algorithm for detecting unlawful bitcoin transactions in the proposed system, according to experiments.

f) CATBOOST

Gradient boosting method CATBOOST is tailored for categorical features and prediction bias correction. It reduces overfitting and improves model stability using ordered boosting and novel encoding. CATBOOST handles transaction types and address-related indicators well in blockchain transaction analysis. Its broad generalization allows it to detect changing laundering trends across transaction circumstances. CATBOOST promotes system robustness by complementing other boosting models.

4. EXPERIMENTAL RESULTS

To test advanced boosting and hybrid machine learning models for money laundering detection, the suggested method was tested on the Elliptic Bitcoin Dataset. After missing value management, numeric conversion, and standard normalisation, the dataset was split into 80% training and 20% testing. Performance was measured by accuracy, precision, recall, F1-score, and confusion matrix. Random Forest, XGBOOST, and ADABOOST were good classification models before the modification, but it improved them. The inclusion of VTAC improves high-frequency and multilayer transaction pattern recognition, enhancing unlawful transaction recall.

By balancing bias and variance, the hybrid XGBOOST–Random Forest model outperformed individual classifiers. Advanced boosting algorithms yielded the greatest benefits. LIGHTGBM outperformed standard and hybrid models with 99.85% detection accuracy, while CATBOOST showed good generalization and stability. These findings demonstrate that improved boosting methods can handle huge, complicated, and uneven blockchain transaction data. Experimental results show that the suggested improvement enhances detection accuracy, scalability, and resilience, making it appropriate for blockchain-based anti-money laundering and crypto compliance applications.

Accuracy: The ability of a test to differentiate between healthy and sick instances is a measure of its accuracy. Find the proportion of analysed cases with true positives and true negatives to get a sense of the test's accuracy. Based on the calculations:

Accuracy = TP + TN /(TP + TN + FP + FN)

$$Accuracy = \frac{(TN + TP)}{T}$$

Precision: The accuracy rate of a classification or number of positive cases is known as precision. Accuracy is determined by applying the following formula:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

$$\Pr e\,cision = \frac{TP}{(TP + FP)}$$

Recall: The recall of a model is a measure of its capacity to identify all occurrences of a relevant machine learning class. A model's ability to detect class instances is shown by the ratio of correctly predicted positive observations to the total number of positives.

$$Recall = \frac{TP}{(FN + TP)}$$

mAP: One ranking quality statistic is Mean Average Precision (MAP). It takes into account the quantity of pertinent suggestions and where they are on the list. The arithmetic mean of the Average Precision (AP) at K for each user or query is used to compute MAP at K.

$$mAP = \frac{1}{n}\sum_{k=1}^{k=n} AP_k$$

$$AP_k = \text{the AP of class } k$$

$$n = \text{the number of classes}$$

F1-Score: A high F1 score indicates that a machine learning model is accurate. Improving model accuracy by integrating recall and precision. How often a model gets a dataset prediction right is measured by the accuracy statistic..

$$F1 = 2 \cdot \frac{(Recall \cdot \Pr e\,cision)}{(Recall + \Pr e\,cision)}$$

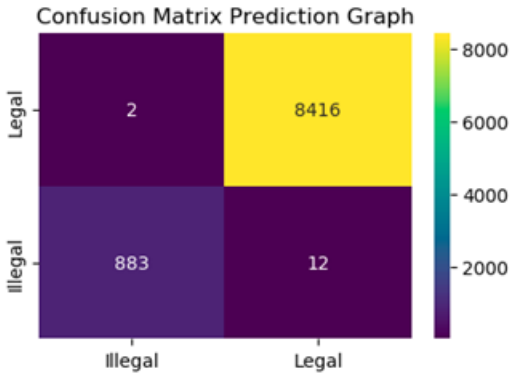

Fig 2 confusion matrix

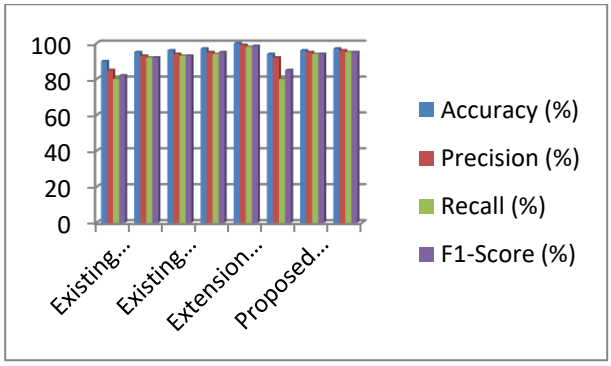

Fig 3 Accuracy graph

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Existing ADABOOST	90	85	80	82
Existing Random Forest	95	93	92	92
Existing XGBOOST	96	94	93	93
Extension Hybrid Model	97	95	94	95
Extension LIGHTGBM	99.85	99	98	98.5

Proposed ADABOOST	94	92	80	85
Proposed Random Forest	96	95	94	94
Proposed XGBOOST	97	96	95	95

Table 1 Accuracy table

5. CONCLUSION

This study extends traditional methods with sophisticated boosting and hybrid models to propose an improved machine learning framework for identifying money laundering activities in blockchain-based cryptocurrency transactions. The solution successfully catches high-frequency, layered, and sophisticated transaction patterns linked to illegal activity by combining machine learning with Value-driven Transactional Analytics for Crypto Compliance (VTAC). Advanced boosting algorithms, especially LIGHTGBM, perform noticeably better than conventional and hybrid models, providing improved accuracy, scalability, and robustness, according to experimental results on the Elliptic Bitcoin Dataset. The results demonstrate that the suggested modification addresses the shortcomings of current AML systems and improves the detection of developing cryptocurrency-based financial crimes while offering a dependable and effective solution for real-world blockchain compliance and anti-money laundering applications.

6. FUTURE SCOPE

The proposed system can be further enhanced by extending its applicability beyond Bitcoin to support multiple cryptocurrencies such as Ethereum and privacy-focused coins like Monero, enabling broader blockchain compliance monitoring. Future work can incorporate deep learning and graph-based models such as Graph Neural Networks (GNNs) to better capture complex relationships between wallet addresses and transaction networks. Additionally, integrating real-time streaming data processing and deployment on distributed or cloud-based platforms can improve scalability and enable live transaction monitoring. The system can also be enhanced with explainable AI techniques to improve transparency and trust in predictions, along with integration of regulatory frameworks and automated alert systems for practical adoption in financial institutions and cybersecurity applications.

REFERENCES

[1] J. Besenyõ and A. Gulyas, ‘‘The effect of the dark web on the security,’’ J. Secur. Sustainability Issues, vol. 11, no. 1, pp. 103–121, Mar. 2021.

[2] C.-Y. Lin, H.-K. Liao, and F.-C. Tsai, ‘‘A systematic review of detecting illicit Bitcoin transactions,’’ Proc. Comput. Sci., vol. 207, pp. 3217–3225, Jan. 2022.

[3] L. Y. Qian. (Oct. 23, 2023). Most Damaging Methods of Crypto Hacks and Exploits in 2022. [Online]. Available: https://www.coingecko. com/research/publications/crypto-hacks-exploits-by-method

[4] J. Gayta. (Nov. 1, 2023). Is It Possible to Hack Cryptocurrency? [Online]. Available: https://www.coingecko.com/research/publications/cryptohacks-exploits-by-method

[5] J. Golosova and A. Romanovs, ‘‘The advantages and disadvantages of the

blockchain technology,'' in Proc. IEEE 6th Workshop Adv. Inf., Electron. Electr. Eng., Nov. 2018, pp. 1–6.

[6] E. Ben Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, ''Zerocash: Decentralized anonymous payments from Bitcoin,'' in Proc. IEEE Symp. Secur. Privacy, May 2014, pp. 459–474.

[7] Y. Li, G. Yang, W. Susilo, Y. Yu, M. H. Au, and D. Liu, ''Traceable monero: Anonymous cryptocurrency with enhanced accountability,'' IEEE Trans. Dependable Secure Comput., vol. 18, no. 2, pp. 679–691, Mar. 2021.

[8] S. Foley, J. R. Karlsen, and T. J. Putniš, ''Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies?'' Rev. Financial Stud., vol. 32, no. 5, pp. 1798–1853, May 2019.

[9] M. Liu, H. Chen, and J. Yan, ''Detecting roles of money laundering in Bitcoin mixing transactions: A goal modeling and mining framework,'' Frontiers Phys., vol. 9, Jul. 2021, Art. no. 665399.

[10] A. Mooij, ''Currency (layering),'' in Regulating the Metaverse Economy: How to Prevent Money Laundering and the Financing of Terrorism. Berlin, Germany: Springer, 2023, pp. 69–86.

[11] B. Moslavac, ''Cryptocurrency tumbler: Legality, legalization, criminalization,'' Revista Acadêmica Escola Superior do Ministério Péblico do Ceará, vol. 11, no. 2, pp. 205–226, Dec. 2019.

[12] J. Crawford and Y. Guan, ''Knowing your Bitcoin customer: Money laundering in the Bitcoin economy,'' in Proc. 13th Int. Conf. Systematic Approaches to Digit. Forensic Eng. (SADFE), May 2020, pp. 38–45.

[13] A. Wahrstätter, J. Gomes, S. Khan, and D. Svetinovic, ''Improving cryptocurrency crime detection: CoinJoin community detection approach,'' IEEE Trans. Dependable Secure Comput., vol. 20, no. 6, pp. 4946–4956, Nov./Dec. 2023.

[14] M. M. Rathore, S. Chaurasia, and D. Shukla, ''Mixers detection in Bitcoin network: A step towards detecting money laundering in cryptocurrencies,'' in Proc. IEEE Int. Conf. Big Data, Dec. 2022, pp. 5775–5782.

[15] A. Shojaeinasab, A. P. Motamed, and B. Bahrak, ''Mixing detection on Bitcoin transactions using statistical patterns,'' IET Blockchain, vol. 3, no. 3, pp. 136–148, Sep. 2023.

[16] Y. Hu, S. Seneviratne, K. Thilakarathna, K. Fukuda, and A. Seneviratne, ''Characterizing and detecting money laundering activities on the Bitcoin network,'' 2019, arXiv:1912.12060.

[17] I. Alarab, S. Prakoonwit, and M. I. Nacer, ''Competence of graph convolutional networks for anti-money laundering in Bitcoin blockchain,'' in Proc. 5th Int. Conf. Mach. Learn. Technol., Jun. 2020, pp. 23–27.

[18] Z. Huang, Y. Huang, P. Qian, J. Chen, and Q. He, ''Demystifying Bitcoin address behavior via graph neural networks,'' in

Proc. IEEE 39th Int. Conf. Data Eng. (ICDE), Apr. 2023, pp. 1747–1760.

[19] N. Lu, Y. Chang, W. Shi, and K. R. Choo, ‘‘CoinLayering: An efficient coin mixing scheme for large scale Bitcoin transactions,’’ IEEE Trans. Dependable Secure Comput., vol. 19, no. 3, pp. 1974–1987, May 2022.

[20] R. I. T. Jensen and A. Iosifidis, ‘‘Fighting money laundering with statistics and machine learning,’’ IEEE Access, vol. 11, pp. 8889–8903, 2023.

[21] J. Alotibi, B. Almutanni, T. Alsubait, H. Alhakami, and A. Baz, ‘‘Money laundering detection using machine learning and deep learning,’’ Int. J. Adv. Comput. Sci. Appl., vol. 13, no. 10, pp. 732–738, 2022.

[22] C. Lee, S. Maharjan, K. Ko, and J. W.-K. Hong, ‘‘Toward detecting illegal transactions on Bitcoin using machine-learning methods,’’ in Proc. 1st Int. Conf. Blockchain Trustworthy Syst., Guangzhou, China. Singapore: Springer, Dec. 2020, pp. 520–533.

[23] M. Jullum, A. Løland, R. B. Huseby, G. Ånonsen, and J. Lorentzen, ‘‘Detecting money laundering transactions with machine learning,’’ J. Money Laundering Control, vol. 23, no. 1, pp. 173–186, Jan. 2020.

[24] E. Pettersson Ruiz and J. Angelis, ‘‘Combating money laundering with machine learning—Applicability of supervised-learning algorithms at cryptocurrency exchanges,’’ J. Money Laundering Control, vol. 25, no. 4, pp. 766–778, Oct. 2022.

[25] J. Lorenz, M. I. Silva, D. Aparício, J. T. Ascensão, and P. Bizarro, ‘‘Machine learning methods to detect money laundering in the Bitcoin blockchain in the presence of label scarcity,’’ in Proc. 1st ACM Int. Conf. AI Finance, Oct. 2020, pp. 1–8.

[26] J. S. Lorenz, ‘‘Machine learning methods to detect money laundering in the Bitcoin blockchain in the presence of label scarcity,’’ Ph.D. thesis, NOVA Inf. Manage. School, NOVA Univ. Lisbon, Lisbon, Portugal, 2021.

[27] C. Leuprecht, C. Jenkins, and R. Hamilton, ‘‘Virtual money laundering: Policy implications of the proliferation in the illicit use of cryptocurrency,’’ J. Financial Crime, vol. 30, no. 4, pp. 1036–1054, May 2023.

[28] M. S. Raza, Q. Zhan, and S. Rubab, ‘‘Role of money mules in money laundering and financial crimes a discussion through case studies,’’ J. Financial Crime, vol. 27, no. 3, pp. 911–931, Oct. 2020.

[29] M. I. A. Rani, S. N. F. S. M. Nazri, and S. Zolkaflil, ‘‘A systematic literature review of money mule: Its roles, recruitment and awareness,’’ J. Financial Crime, vol. 31, no. 2, pp. 347–361, Mar. 2024.

[30] C. Wronka, ‘‘‘Cyber-laundering’: The change of money laundering in the digital age,’’ J. Money Laundering Control, vol. 25, no. 2, pp. 330–344, 2022