Mr.B. Mohan, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Machine Learning in Money Laundering Detection Over Blockchain Technology

Mr.B. Mohan[1], Marthala Muni Namitha[2], Palloli Veera Vyshnavi[3], Neelam Venkata Vamsi[4]

[1]Professor, Department of CSE, Sai Rajeswari Institute of Technology, Proddatur-516362, Andhra Pradesh, India.
[2,3,4]UG Students,Department of Computer Science &Engineering,Sai Rajeswari Institute of Technology,Proddatur-516362,AndhraPradesh,India.

Abstract- Layering through cryptocurrency transactions represents a sophisticated mechanism for laundering money within cybercrime circles. This process methodically merges illegal funds into the legitimate financial system. Blockchain technology plays a crucial role in this integration by facilitating the quick and automated dispersal of assets across various digital wallets and exchanges. Machine learning emerges as a powerful tool for analyzing and identifying illicit transactions within Blockchain networks; however, a significant challenge remains in the form of a gap in advanced pattern recognition algorithms. This paper introduces a novel machine learning-based approach called Value-driven-Transactional tracking Analytics for Crypto compliance (VTAC) for the detection of illegal crypto transactions via Blockchain. The approach combines machine learning algorithms with a pre-training process, normalization, model training, and a de-anonymization process to analyze and identify illicit transactions effectively. Experimental evaluations show VTAC's capability to detect illegal transactions with a 97.5% accuracy using the XG Boost model, outperforming existing methods with an accuracy of up to 95.9%. Key performance metrics, including precision, recall, and F1-score, consistently exceeded 95%, highlighting VTAC's enhanced precision and reliability. The proposed solution will serve as an advisory framework to help financial crime investigators enhance the detection and reporting of suspicious cryptocurrency transactions in cyberspace.

Keywords: Machine learning, blockchain, cybercrime, cryptocurrency, money laundering.

I. INTRODUCTION

Crypto currencies are the most widely used in criminal activity for money laundering, fraud, theft, and carrying out dark web deals such as drug trafficking, weapon sales, and the sale of stolenpersonalinformation. Crypto currencies facilitate a shadow economy on the dark web, allowing the purchase and sale of illicit goods and services without the oversight of regulatory bodies. Criminals use crypto currencies to hide the proceeds of their illegal activities . Cybercriminals can use deceptive tactics like phishing, social engineering, or investment scams to trick individuals and persuade them to transfer their cryptocurrencies to malicious entities. Cybercriminals might pose as legitimate businesses or create fake investment opportunities.

Objective

The objective of this project is to identify suspicious financial activities such as money laundering by examining key transaction features including wallet addresses, transaction values, frequency, and time patterns.

The system aims to leverage powerful machine learning algorithms like Random Forest, AdaBoost, and XGBoost to classify transactions as legal or illegal with high accuracy. Additionally, the project focuses on tracking transaction flows and uncovering hidden patterns that are difficult to detect using traditional methods.

By integrating data preprocessing, normalization, and model training techniques, the proposed system ensures efficient handling of large-scale blockchain data. The ultimate goal is to enhance security, transparency, and trust in cryptocurrency systems while supporting financial investigators and regulatory authorities in preventing cybercrime and ensuring compliance with anti-money laundering regulations.

Problemstatement

The increasing adoption of cryptocurrency and blockchain technology has significantly amplified the risk of money laundering activities in digital financial systems. The inherent characteristics of blockchain, such as decentralization, anonymity, and lack of centralized control, make it difficult for traditional Anti-Money Laundering (AML) systems to effectively trace and identify illicit transactions. Existing detection approaches, primarily based on rule-based methods and conventional machine learning techniques, are limited in capturing complex transactional relationships and often fail to adapt to evolving laundering patterns.Moreover, the presence of highly imbalanced datasets and the use of sophisticated obfuscation techniques, such as transaction mixing and layering, further degrade detection accuracy and increase false positive rates. These challenges highlight the need for a robust and intelligent framework capable of analyzing large-scale blockchain transaction data, identifying hidden patterns, and detecting suspicious activities with high precision.Therefore, the problem addressed in this work is the design and development of an efficient machine learning-based system that enhances the detection of money laundering activities over blockchain networks while improving accuracy, scalability, and real-time monitoring capabilities.

II. FEASIBILITYSTUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company.For feasibility analysis, some understanding of the major requirements for the system is essential.

TypesofFeasibilityStudy

There are several different kinds of feasibility studies. Understanding the types of feasibility studiesandthetechnicalitiesoftheconceptisimportant foranybusiness.Theyareelaborated below:

TechnicalFeasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

EconomicalFeasibility

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

Social Feasibility

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

III. LITERATURESURVEY

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

The Blockchain is the newest and perspective technology in modern economy. This technology can help to solve different kind of problems in the industrial sphere, such as trust, transparency, security and reliability of data processing. In theory, the use of Blockchain technology shows great and positive results, but what can say about practice? In this

paper the description of the Blockchain technology, and it advantages and disadvantages are analyzed. Many already implemented applications of Blockchain technology were studied, as well as affected success or problems factors during the implementations. This paper aim is to analyze conveniences and difficulties, related to the Blockchain integration and implementation in the different fields of modern industry.

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.

Bit coin is the first digital currency to see widespread adoption. While payments are conducted between pseudonyms, Bit coin cannot offer strong privacy guarantees: payment transactions are recorded in a public decentralized ledger, from which much information can be deduced. Zero coin (Miers et al., IEEE S&P 2013) tackles some of these privacy issues by unlinking transactions from the payment's origin. Yet, it still reveals payments' destinations and amounts, and is limited in functionality. In this paper, we construct a full-fledged ledger-based digital currency with strong privacy guarantees. Our results leverage recent advances in zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs). First, we formulate and construct decentralized anonymous payment schemes (DAP schemes). A DAP scheme enables users to directly pay each other privately: the corresponding transaction hides the payment's origin, destination, and transferred amount. We provide formal definitions and proofs of the construction's security. Second, we build Zero cash, a practical instantiation of our DAP scheme construction. In Zero cash, transactions are less than 1 kB and take under 6 ms to verify - orders of magnitude more efficient than the less-anonymous Zero coin and competitive with plain Bit coin.

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.

Monero provides a high level of anonymity for both users and their transactions. However, many criminal activities might be committed with the protection of anonymity in cryptocurrency transactions. Thus, user accountability (or traceability) is also important in Monero transactions, which is unfortunately lacking in the current literature. In this paper, we fill this gap by introducing a new cryptocurrency named Traceable Monero to balance the user anonymity and accountability. Our framework relies on a tracing authority, but is optimistic, in that it is only involved when investigations in certain transactions are required. We formalize the system model and security model of Traceable Monero. We present a detailed construction of Traceable Monero by overlaying Monero with two types of tracing mechanisms, tracing the one-time addresses with money flows and tracing the long-term addresses. We prove the security of Traceable Monero and implement a prototype of the system, which demonstrates that Traceable Monero incurs merely a very small overhead in generating and verifying a transaction compared to Monero transactions.

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.

Cryptocurrencies, particularly Bitcoin, have garnered attention for their potential in anonymous transactions. However, their anonymity has often been compromised by deanonymization attacks. To counter this, mixing services have been introduced. While they enhance privacy, they obscure fund traceability. This study seeks to demystify transactions linked to these services, shedding light on pathways of concealed and laundered money. We propose a method to identify and classify transactions and addresses of major mixing services in Bitcoin. Unlike previous research focusing on older techniques like CoinJoin, we emphasize modern mixing services. We gathered labelled data by transacting with three prominent mixers (MixTum,

Blemder, and CryptoMixer) and identified recurring patterns. Using these patterns, an algorithm was created to pinpoint mixing transactions and distinguish mixer-related addresses.

The algorithm achieved a remarkable recall rate of 100%. Given the lack of clear ground truth and the vast number of unlabelled transactions, ensuring accuracy was a challenge. However, by analyzing a set of non-mixing transactions with our model, it was confirmed that the high recall rate was not misleading. This work provides a significant advancement in monitoring mixing transactions, presenting a valuable tool against fraud and money laundering in cryptocurrency networks.

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

Money laundering is a profound global problem. Nonetheless, there is little scientific literature on statistical and machine learning methods for anti-money laundering. In this paper, we focus on anti-money laundering in banks and provide an introduction and review of the literature. We propose a unifying terminology with two central elements(i) client risk profiling and (ii) suspicious behavior flagging. We find that client risk profiling is characterized by diagnostics, i.e., efforts to find and explain risk factors. On the other hand, suspicious behavior flagging is characterized by non-disclosed features and hand-crafted risk indices. Finally, we discuss directions for future research. One major challenge is the need for more public data sets. This may potentially be addressed by synthetic data generation. Other possible research directions include semi-supervised and deep learning, interpretability, and fairness of the results.

IV. EXISTINGSYSTEM

Existing systems for detecting money laundering in financial and blockchain environments primarily rely on rule-based approaches and traditional machine learning techniques. These systems use predefined rules, thresholds, and historical transaction patterns to identify suspicious activities. In blockchain networks, some methods focus on statistical analysis, transaction tracing, and identification of mixing services to detect illicit behavior.

Several approaches utilize machine learning models such as decision trees, support vector machines, and clustering techniques to classify transactions as legitimate or suspicious. A research study in investigates the application of Graph Convolutional Networks (GCN) for identifying unauthorized transactions within the Bitcoin network. The work presents an innovative method that integrates GCN with linear layers, with the goal of enhancing the accuracy of forecasting illegal transactions. The performance of this strategy is assessed using the Elliptic dataset and exhibits enhanced efficacy in comparison to GCN models employed in prior studies.

The authors in commence by emphasizing the significance of comprehending Bitcoin address patterns inside the anonymous framework of the Blockchain. They proposed their BAClassifier system, which includes address graph building, graph representation learning, and address classification with graph neural networks. The main improvements consist of a technique for creating chronological transaction graphs and an efficient data-driven method for effectively acquiring these representations.

DisadvantagesofExistingSystem:

- **The complexity of data:** Most of the existing machine learning models must be able to accurately interpret large and complex datasets for Money Laundering Detection.
- **Data availability:** Most machine learning models require large amounts of data to create accurate predictions. If data is unavailable in sufficient quantities, then model accuracy may suffer.
- **Incorrect labeling:** The existing machine learning models are only as accurate as the data trained using the input dataset. If the data has been incorrectly labeled, the model cannot make accurate predictions.

Systemarchitecture

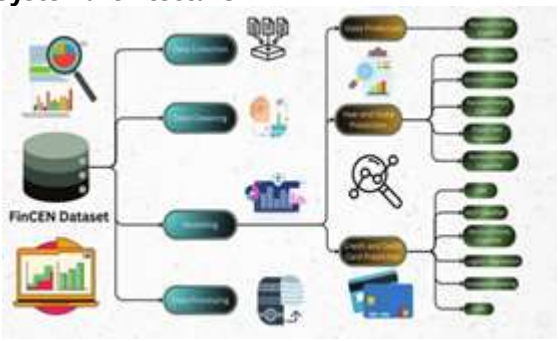

Fig.4.1SystemArchitecture

IMPLEMENTATION MODULES

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Upload Datasets Train & Test Datasets, View Trained and Tested Datasets Accuracy in Bar Chart, View Trained and Tested Datasets Accuracy Results, View Detection Of Money Laundering Details, View All Uploaded Datasets, Download Predicted Data Sets, View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations likeREGISTER AND LOGIN, Detection Of Money Laundering Status , View Your Profile.

Applying Machine Learning

A notable challenge in the training of machine learning models, especially evident in the realm of financial analytics, is the occurrence of data leakage during the normalization process. This problem often arises when the normalization model incorporates data from both the training and test datasets. Particularly, observations from the test data, which should ideally remain separate and unknown during the training phase, inadvertently influence the normalization parameters. This mishap results in the test data influencing the normalized training samples and, subsequently, thetrained model itself. Moreover, the conventional practice of splitting the data into only two sets—training and test—rather than three distinct sets (training, validation, and test) exacerbates this issue. In such scenarios, the test data inadvertently participates in model selection and validation processes, further compounding the risk of data leakage.

Outcome

The dataset upload module was successfully executed. The system allows the user to upload transaction data in CSV format This ensures that real-world financial data can be used for training the machine learning models.

The system successfully trained multiple machine learning models using the uploaded dataset. The output displays accuracy, classification report, and confusion matrix for each model. This helps in evaluating the performance of different algorithms.
The uploaded dataset is displayed in a structured tabular format. Each record contains transaction details such as sender account, receiver account, amount, and transaction type. This output confirms that the data has been correctly loaded and is ready for preprocessing and model training.

The graphical representation compares the accuracy of different machine learning models. It is observed that the Gradient Boosting Classifier achieved higher accuracy compared to other models such as SVM and Logistic Regression. This helps in selecting the best model for prediction.

V. CONCLUSION

The study demonstrates that integrating Machine Learning techniques into Anti-Money Laundering (AML) systems significantly improves the detection of suspicious financial transactions. Traditional rule-based systems are limited in identifying complex and evolving laundering patterns, often resulting in high false positive rates and heavy manual intervention.

The proposed ML-based framework effectively analyzes transaction behavior, extracts meaningful features, and classifies transactions using supervised and anomaly detection approaches. The experimental results indicate improved detection accuracy, better recall of suspicious cases, and enhanced risk scoring capability.

The system is scalable, adaptable to new laundering strategies, and capable of supporting regulatory compliance requirements. Overall, the research confirms that machine learning provides a robust and intelligent solution for modern financial crime detection systems.

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 detectingillicit Bitcoin transactions,'' Proc. Comput. Sci., vol. 207, pp. 3217–3225,Jan. 2022.
3. L. Y. Qian. (Oct. 23, 2023). Most Damaging Methods of CryptoHacks 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
4. J. Golosova and A. Romanovs, ''The advantages and disadvantages of theblockchain technology,'' in Proc. IEEE 6th Workshop Adv. Inf., Electron.Electr. Eng., Nov. 2018, pp. 1–6.
5. E. Ben Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, andM. Virza, ''Zerocash: Decentralized anonymous payments from Bitcoin,''in Proc. IEEE Symp. Secur. Privacy, May 2014, pp. 459–474.
6. 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.
7. S. Foley, J. R. Karlsen, and T. J. Putniš, ''Sex, drugs, and Bitcoin: Howmuch illegal activity is financed through cryptocurrencies?'' Rev. FinancialStud., vol. 32, no. 5, pp. 1798–1853, May 2019.
8. M. Liu, H. Chen, and J. Yan, ''Detecting roles of money laundering inBitcoin mixing transactions: A goal modeling and mining framework,''Frontiers Phys., vol. 9, Jul. 2021, Art. no. 665399.
9. 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.
10. B. Moslavac, ''Cryptocurrency tumbler: Legality, legalization, criminalization,''RevistaAcadĕmica Escola Superior do MinistérioPéblico doCeará, vol. 11, no. 2, pp. 205–226, Dec. 2019.
11. J. Crawford and Y. Guan, ''Knowing your Bitcoin customer: Moneylaundering in the Bitcoin economy,'' in Proc. 13th Int. Conf. SystematicApproaches to Digit. Forensic Eng. (SADFE), May 2020, pp. 38–45.
12. A. Wahrstätter, J. Gomes, S. Khan, and D. Svetinovic, ''Improving cryptocurrencycrime detection: CoinJoin community detection approach,''IEEE Trans. Dependable Secure Comput., vol. 20, no. 6, pp. 4946–4956,Nov./Dec. 2023.
13. M. M. Rathore, S. Chaurasia, and D. Shukla, ''Mixers detection inBitcoin network: A step towards detecting money laundering in cryptocurrencies,''in Proc. IEEE Int. Conf. Big Data, Dec. 2022, pp. 5775–5782.
14. A. Shojaeinasab, A. P. Motamed, and B. Bahrak, ''Mixing detection onBitcoin transactions using statistical patterns,'' IET Blockchain, vol. 3,no. 3, pp. 136–148, Sep. 2023.
15. Y. Hu, S. Seneviratne, K. Thilakarathna, K. Fukuda, and A. Seneviratne,''Characterizing and detecting money laundering activities on the Bitcoinnetwork,'' 2019, arXiv:1912.12060.
16. I. Alarab, S. Prakoonwit, and M. I. Nacer, ''Competence of graphconvolutional networks for anti-money laundering in Bitcoin blockchain,''in Proc. 5th Int. Conf. Mach. Learn. Technol., Jun. 2020, pp. 23–27.
17. Z. Huang, Y. Huang, P. Qian, J. Chen, and Q. He, ''Demystifying Bitcoinaddress behavior via graph

neural networks,'' in Proc. IEEE 39th Int. Conf.Data Eng. (ICDE), Apr. 2023, pp. 1747–1760.
18. N. Lu, Y. Chang, W. Shi, and K. R. Choo, ''CoinLayering: An efficientcoin mixing scheme for large scale Bitcoin transactions,'' IEEE Trans.Dependable Secure Comput., vol. 19, no. 3, pp. 1974–1987, May 2022.
19. R. I. T. Jensen and A. Iosifidis, ''Fighting money laundering with statisticsand machine learning,'' IEEE Access, vol. 11, pp. 8889–8903, 2023.
20. J. Alotibi, B. Almutanni, T. Alsubait, H. Alhakami, and A. Baz, ''Moneylaundering detection using machine learning and deep learning,'' Int. J.Adv. Comput. Sci. Appl., vol. 13, no. 10, pp. 732–738, 2022.
21. C. Lee, S. Maharjan, K. Ko, and J.W.-K. Hong, ''Toward detecting illegaltransactions on Bitcoin using machine-learning methods,'' in Proc. 1stInt. Conf. Blockchain Trustworthy Syst., Guangzhou, China. Singapore:Springer, Dec. 2020, pp. 520–533.
22. 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.
23. E. Pettersson Ruiz and J. Angelis, ''Combating money laundering withmachine learning—Applicability of supervised-learning algorithms atcryptocurrency 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 Bitcoinblockchain in the presence of label scarcity,'' in Proc. 1st ACM Int. Conf.AI Finance, Oct. 2020, pp. 1–8.