International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 2, 2026

A Robust VTAC-Assisted Machine Learning Framework for Money Laundering Detection in Block chain Systems

Ranapratap Pola[1],**B. Ganga Bhavani**[2]

[1]M. Tech PG Scholar; Department of CSE BVC Engineering College, Odalarevu Andhra Pradesh, India.

[2]Associate Professor; Department of CSE BVC Engineering College, Odalarevu Andhra Pradesh, India.

Mail Id; Polaranapratap7@gmail.com,bgangabhavani.bvce@bvcgroup.in

Abstract

Money laundering through bitcoin transactions has grown to be a significant issue due to the decentralized and pseudonymous nature of blockchain networks. Traditional machine learning methods for identifying illegal transactions often have limited accuracy and poor generalization when working with large and complex transaction datasets. In order to get over these limitations, this study proposes an enhanced money laundering detection system that uses advanced boosting and hybrid machine learning methods. The system uses a hybrid model that combines powerful boosting algorithms like LIGHTGBM and CATBOOST with XGBOOST and Random Forest to improve detecting capabilities. Value-driven Transactional Analytics for Crypto Compliance (VTAC) is utilized to identify high-frequency, multilayer transaction patterns that are often associated with money laundering. Experimental evaluation on the Elliptic Bitcoin Dataset demonstrates that the proposed approach significantly improves prediction performance, with LIGHTGBM achieving the highest accuracy of 99.85%. Since the results confirm that advanced boosting and hybrid models provide better accuracy, scalability, and resilience, the recommended technique is very effective 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*

INTRODUCTION

By facilitating decentralized, transparent, and peer-to-peer transactions, the quick development of blockchain technology and cryptocurrencies has drastically changed digital financial systems. Although these features improve efficiency and security, they have also raised significant security issues. The usage of cryptocurrencies for illicit purposes, including money laundering, drug trafficking, ransomware payments, arms dealing, and the selling of stolen personal data, has increased since the dark web emerged. Cryptocurrencies have emerged as a popular means for hackers to transfer illegal cash anonymously because to the lack of centralized control and regulatory scrutiny, posing a serious danger to global financial security [1].

Because of its widespread acceptability, liquidity, and popularity among cryptocurrencies, Bitcoin has been used extensively for illicit financial transactions. A substantial percentage of bitcoin transactions are associated with illegal activity, according to several studies, underscoring the critical need for efficient detection methods [2]. Despite the fact that blockchain transactions are publicly documented, it is challenging to immediately link transactions to actual people due to the pseudonymous nature of wallet addresses. This restriction makes it more difficult to execute standard anti-money laundering (AML) laws by enabling criminals to conceal money flows using methods like transaction chaining, mixing services, and tumblers.

The money laundering issue has gotten worse in recent years due to the rise in cryptocurrency breaches, phishing scams, and exploit-based crimes. Cybercriminals frequently take advantage of flaws in wallets, exchanges, and smart contracts to steal digital assets, which are subsequently laundered through intricate transaction patterns across several addresses and platforms [3]. The increasing complexity of illegal financial activities inside blockchain ecosystems is highlighted by reports that billions of dollars have been lost as a result of cryptocurrency-related breaches [4]. Intelligent and adaptive detection systems that can recognize suspicious actions beyond basic rule-based monitoring are necessary in light of these developing assault methods.

Blockchain technology has both advantages and disadvantages when it comes to financial security, despite its creative design. Although immutability and openness are significant benefits, a significant disadvantage for crime prevention is the absence of built-in identity verification systems and regulatory enforcement [5]. The majority of current AML systems rely on graph-based or classical machine learning techniques, which frequently have issues with scalability, unbalanced data, and changing money 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. This paper suggests an improved money laundering detection framework that expands on current methods by incorporating sophisticated boosting and hybrid machine learning techniques in order to get over these restrictions. The suggested method enhances prediction accuracy, scalability, and resilience by fusing cutting-edge boosting algorithms like LIGHTGBM with potent ensemble models like XGBOOST–Random Forest hybrids. Furthermore, transaction value and frequency patterns are analyzed using Value-driven Transactional Analytics for Crypto Compliance (VTAC), which makes it possible to identify sophisticated laundering operations more successfully. For blockchain-based AML and crypto compliance monitoring, this integrated method offers a scalable and high-performance solution.

LITERATURE SURVEY

a)Enhancing Anti-Money Laundering Frameworks: An Application of Graph Neural Networks in Cryptocurrency Transaction Classification:

Money laundering via cryptocurrencies is a serious problem as it not only makes illegal activity easier to commit and conceal, but it also disturbs markets and the financial system as a whole. Researchers are working to create strong Anti-Money Laundering (AML) frameworks in order to address this dilemma. By lessening the effects of criminal activity, these initiatives are essential to advancing public wellbeing. The use of Graph Neural Networks (GNNs) for Bitcoin transaction classification is investigated in this research. In particular, the study makes use of GraphSAGE networks, Chebyshev spatial convolutional neural networks, Graph Convolutional Networks (GCNs), and Graph Attention Networks (GATs). We experiment with various feature subsets based on the dataset analysis. Our results imply that the state-of-the-art outcomes can be improved by using Graph Neural Network convolutions in conjunction with a final linear layer and skip connections, particularly when Chebyshev and GATv2 convolutions are employed.

b)Exploring the Effectiveness of Machine Learning Models in Detecting Anomalous Transactions

Illegal financial flows and money laundering support criminal activity and jeopardize economic stability. Because they are decentralized and anonymous, cryptocurrencies pose regulatory issues. Financial transactions that depart from known trends and may indicate fraud, mistakes, or unexpected conduct are referred to as anomalous transactions. From the standpoint of anti-money laundering/counter-terrorist financing (AML/CFT), this study examines machine learning methods for identifying unusual bitcoin transactions. For our investigation, a dataset of actual Bitcoin transactions is examined. The effectiveness of several machine learning models in identifying unusual transactions is evaluated in this research. In order to stop fraud in sectors like banking, e-commerce, and financial services, it is critical to identify these irregularities.

c)Group-Based Detection of Cryptocurrency Laundering Using Multi-Persona Analysis:

The blockchain ecosystem is being threatened by cryptocurrency-based money laundering. It is challenging to identify such money laundering operations since cryptocurrencies are decentralized and anonymous. Even though a lot of research has been done, practically all current techniques identify bitcoin laundering from an individual standpoint, neglecting the reality that money laundering is usually a collective activity. The study of laundering activity should benefit greatly from group knowledge, however the secrecy and variety of reasons of bitcoin transactions make it difficult to identify such laundering groups. We create a multi-persona grouping algorithm that successfully groups accounts into persona subgraphs in order to overcome this difficulty. Next, we create an unsupervised model to assess each subgraph's laundering score by extracting two subgraph features: cycle basis number and cycle overlapping ratio. Our suggested approach can increase detection accuracy by an average of 17.4 percentage points when compared to current approaches, according to extensive studies conducted on both synthetic and real-world datasets. As far as we are aware, this is the first study on group-based bitcoin laundering detection.

d)Deep Learning for Cross-Border Transaction Anomaly Detection in Anti-Money Laundering Systems

Anti-money laundering (AML) has emerged as a critical component of financial supervision, especially in cross-border transactions, in light of globalization and the fast growth of the digital economy. In order to counteract more sophisticated money laundering strategies, more intelligent and adaptable AML systems are required due to the growing complexity and scope of international financial transactions. With an emphasis on rule optimization utilizing contrastive learning approaches, this study investigates the use of unsupervised learning models in cross-border AML systems. To evaluate their effectiveness in identifying anomalous transactions, five deep learning models were created and evaluated, ranging from simple convolutional neural networks (CNNs) to hybrid CNN-GRU architectures. The findings show that the detection accuracy and responsiveness of the system increase with model complexity. Specifically, the

accuracy and area under the receiver operating characteristic curve (AUROC) of the self-developed hybrid Convolutional-Recurrent Neural Integration Model (CRNIM) model demonstrated higher performance. These results demonstrate how unsupervised learning models may greatly enhance AML systems' intelligence, adaptability, and real-time capabilities. This study contributes both theoretically and practically to the development of AML technologies, which are crucial for protecting the global financial system against illegal activity, by improving adaptation to new money laundering methods and optimizing detection standards.

e)GCF-MLD: Integrated Approach for Money Laundering Detection Using Machine Learning and Graph Network Analysis:

Financial institutions face a serious problem with money laundering, particularly in developing nations, and it can be difficult to identify such questionable activity. Financial institutions presently employ rule-based money laundering detection systems that rely on pre-established rules that are frequently unable to keep up with money launderers' quickly evolving strategies. In this context, machine learning-based methods for identifying suspected money laundering transactions have drawn interest. In order to identify suspect accounts in real-world banking datasets, we provide a unique method in this paper called "Graph-Clustering Fusion for Money Laundering Detection (GCF-MLD)" that combines graph network analysis with clustering methodology. The findings show that financial institutions may easily replace existing rule-based methods with the suggested model to greatly increase the efficacy and efficiency of money laundering detection systems.

METHODOLOGY

i) Proposed Work:

By adding sophisticated boosting and hybrid learning techniques to conventional machine learning methods, the proposed project seeks to improve money laundering detection in blockchain-based cryptocurrency transactions. To extract significant transactional aspects such wallet hash behavior, transaction amount, temporal trends, and transaction frequency, the system makes use of amount-driven Transactional Analytics for Crypto Compliance (VTAC). To guarantee high-quality input data, these characteristics are processed through an organized preparation pipeline that includes missing value management, numeric encoding, and standard normalization. To provide a solid foundation for detection performance, machine learning models such as Random Forest, XGBOOST, and ADABOOST are first used to categorize transactions as either lawful or illicit.

The suggested system incorporates hybrid and advanced boosting models as a crucial extension to further enhance accuracy, scalability, and generalization. To take use of the advantages of both gradient boosting and ensemble decision trees, a hybrid model that combines XGBOOST and Random Forest is created. Furthermore, cutting-edge boosting algorithms like LIGHTGBM and CATBOOST are included to effectively manage complicated and large-scale blockchain information. The high-frequency, multilayer, and unusual transaction patterns frequently connected to money laundering are captured by these models. 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:

The system architecture is intended to offer a scalable and effective framework for identifying illegal bitcoin transactions on blockchain networks. Raw bitcoin transaction data, such as sender and recipient wallet hash addresses, transaction value, date, and transaction frequency, is first gathered. This transactional data is sent to the detecting layer after being arranged as crypto transactional data. To provide consistent data representation, the preprocessing module resolves missing values, transforms non-numeric characteristics into numerical form, and performs conventional normalization. Reliable learning is made possible by this organized data preparation, which also lowers noise in later phases of analysis.

Following preprocessing, the machine learning and decision-making layer processes the transaction data, producing prediction results using several ensemble and boosting-based models. This layer is made up of sequential decision structures that examine transactional behavior from several angles. These structures are represented as many 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. The prediction's outcome is generated by the final output module, which identifies illicit transactions together with related wallet hash addresses, incoming and outgoing values, and transaction dates. For blockchain-based anti-money laundering and crypto compliance monitoring systems, this design guarantees precise identification, effective scalability, and useful deployment.

iii) Modules:

a)Transaction Data Collection Module

This module is responsible for collecting raw cryptocurrency transaction details from the blockchain

dataset. It gathers essential attributes such as sender wallet hash, receiver wallet hash, transaction value, transaction date, and transaction frequency. The collected data forms the foundation for further analysis and detection.

b)Data Preprocessing Module

This module cleans and prepares the collected transaction data for machine learning. It handles missing values, converts non-numeric fields into numeric representations, and applies standard scaling for normalization. Proper preprocessing ensures consistent input and improves model accuracy and reliability.

c)VTAC Feature Analysis Module

The Value-driven Transactional Analytics for Crypto compliance (VTAC) module analyzes transaction values, frequency, and temporal patterns. It identifies high-frequency transfers and unusual value movements that are indicative of money laundering behavior. This module enhances feature representation for effective detection.

d)Machine Learning and Hybrid Modeling Module

This module implements machine learning algorithms such as Random Forest, XGBOOST, and ADABOOST, along with hybrid and advanced boosting models including XGBOOST–Random Forest, LIGHTGBM, and CATBOOST. It trains these models to classify transactions as legal or illegal based on learned patterns.

e)Prediction Selection Module

The prediction selection module aggregates outputs from multiple models and decision trees. It evaluates the confidence of each prediction and selects the most accurate classification outcome. This ensemble-based decision mechanism improves robustness and reduces false positives.

f)Result and Reporting Module

This module presents the final prediction results, identifying illegal transactions and associated wallet hash addresses. It displays incoming and outgoing transaction values along with corresponding dates. The results support effective monitoring, investigation, and enforcement for blockchain-based anti-money laundering and crypto compliance systems.

iv) Algorithms:

a)Random Forest

Random Forest is an ensemble learning algorithm that constructs multiple decision trees using random subsets of training data and feature sets. Each tree independently learns transaction behavior, and the final prediction is obtained through majority voting. This approach effectively reduces variance and minimizes overfitting, which is crucial for highly imbalanced cryptocurrency transaction datasets. In the proposed system, Random Forest serves as a strong baseline model, capturing general transactional trends such as value distribution, transaction counts, and wallet interaction patterns. Its robustness makes it suitable for initial detection of suspicious transactions.

b)XGBOOST

XGBOOST (Extreme Gradient Boosting) is a powerful gradient boosting algorithm that builds models sequentially by optimizing a differentiable loss function. Each new tree corrects the errors made by previous trees, allowing the model to learn complex non-linear relationships in transaction data. In blockchain AML detection, XGBOOST efficiently captures subtle laundering behaviors such as structured transfers and repeated low-value transactions. Its built-in regularization mechanisms prevent overfitting and improve generalization. The algorithm plays a key role in enhancing prediction accuracy within the proposed framework.

c)ADABOOST

ADABOOST (Adaptive Boosting) is an ensemble method that dynamically adjusts the importance of training samples based on their classification difficulty. Transactions that are misclassified in earlier iterations receive higher weights, forcing the model to focus on rare and suspicious laundering activities. This property makes ADABOOST particularly effective for detecting illegal transactions that occur infrequently compared to legal ones. In the proposed system, ADABOOST improves recall for illicit transactions and strengthens the system's sensitivity to anomalous behavior.

d)Hybrid XGBOOST–Random Forest

The hybrid XGBOOST–Random Forest model combines the complementary strengths of gradient boosting and bagging-based ensembles. XGBOOST excels at learning intricate feature interactions and transaction dependencies, while Random Forest provides stability and resistance to noise. By integrating predictions from both models, the hybrid approach achieves better balance between bias and variance. This hybrid design enhances detection of complex laundering strategies such as layering and rapid fund circulation, making it a key extension over conventional AML models.

e)LIGHTGBM

LIGHTGBM is an advanced gradient boosting framework designed for high efficiency and scalability on large datasets. It employs leaf-wise tree growth and histogram-based splitting to significantly reduce training time while maintaining high accuracy. In the context of blockchain analytics, LIGHTGBM effectively handles high-dimensional transaction features and large volumes of data. Experimental results show that LIGHTGBM achieves the highest detection accuracy in the proposed system, making it

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

the most effective algorithm for identifying illicit cryptocurrency transactions.

f)CATBOOST

CATBOOST is a gradient boosting algorithm specifically optimized to handle categorical features and prevent prediction bias. It uses ordered boosting and innovative encoding techniques to improve model stability and reduce overfitting. In blockchain transaction analysis, CATBOOST effectively processes categorical attributes such as transaction types and address-related indicators. Its strong generalization capability makes it suitable for detecting evolving laundering patterns across different transaction scenarios. CATBOOST complements other boosting models and enhances overall system robustness.

EXPERIMENTAL RESULTS

The Elliptic Bitcoin Dataset, which is accessible to the public, was used in the experimental evaluation of the suggested approach to determine how well advanced boosting and hybrid machine learning models identify money laundering. Following preparation procedures such resolving missing values, converting numbers, and standard normalization, the dataset was split into 80% for training and 20% for testing. Metrics like as accuracy, precision, recall, F1-score, and confusion matrix were used to assess performance. Although baseline models like Random Forest, XGBOOST, and ADABOOST showed good classification capabilities, the suggested extension improved their performance even further. Recall for illegal transactions was greatly increased by the incorporation of VTAC, which allowed for better recognition of high-frequency and multilayer transaction patterns.

By successfully managing bias and variance, the hybrid XGBOOST–Random Forest strategy outperformed individual classifiers among all examined models. But the biggest increases came from the sophisticated boosting algorithms. With an accuracy of 99.85%, LIGHTGBM outperformed both standard and hybrid models in terms of detection performance, while CATBOOST also showed good stability and generalization. These findings demonstrate that sophisticated boosting methods are quite successful in managing complicated, unbalanced, and large-scale blockchain transaction data. The results of the experiment confirm that the suggested expansion greatly increases detection accuracy, scalability, and resilience, which qualifies the system for practical blockchain-based anti-money laundering and crypto compliance applications.

Accuracy: A test's accuracy is its capacity to distinguish healthy from ill cases. Find the percentage of instances with genuine positives and negatives to assess test accuracy.

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

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

Precision: Classification accuracy or positive cases constitute precision. The formula for accuracy is:

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

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

Recall: A model's recall measures its ability to recognize all appropriate machine learning class instances. The ratio of accurately predicted positive observations to total positives indicates a model's class instance detection skill.

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

mAP: Mean Average Precision ranks quality. It considers the number and order of relevant ideas. Calculating MAP at K uses the arithmetic mean of each user or query's Average Precision (AP).

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

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

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

F1-Score: A high F1 score suggests an accurate machine learning model. Integrating recall and precision improves model correctness. Accuracy measures how often a model predicts a dataset correctly.

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

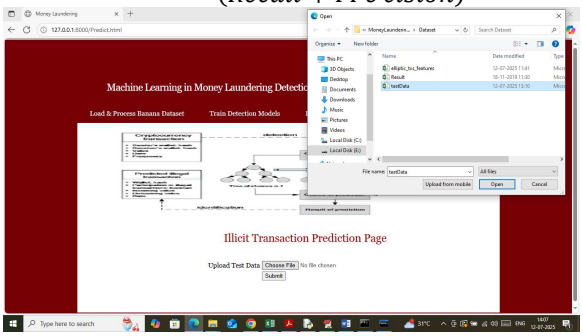

Fig 1 upload input

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

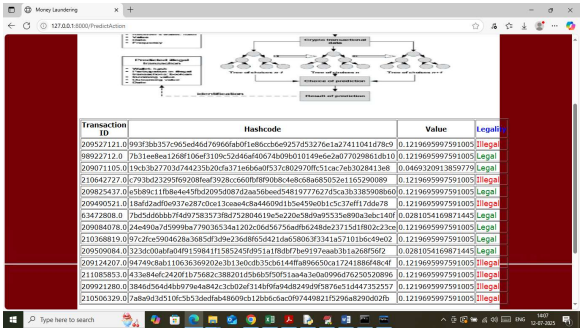

Fig2 results

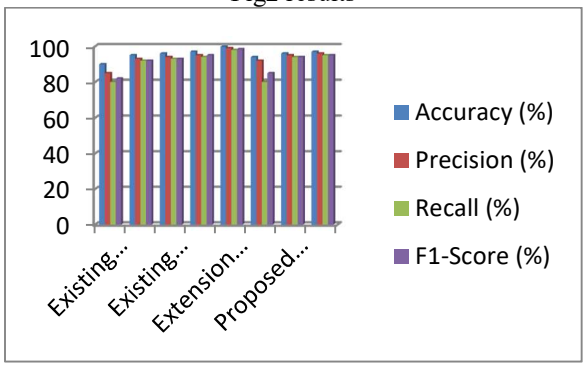

Fig 3 Accuracy graph

CONCLUSION

This work extends traditional methods with sophisticated boosting and hybrid models to provide an improved machine learning framework for identifying money laundering activities in blockchain-based cryptocurrency transactions. The technology 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, greatly outperform conventional and hybrid models, delivering higher accuracy, scalability, and robustness, according to experimental results on the Elliptic Bitcoin Dataset. The results verify that the suggested modification, which addresses the shortcomings of current AML systems and improves the detection of developing cryptocurrency-based financial crimes, offers a dependable and effective solution for practical blockchain compliance and anti-money laundering applications.

FUTURE SCOPE

Future improvements might concentrate on using real-time blockchain monitoring to identify questionable transactions as they happen. The technology will be more applicable in a variety of financial ecosystems if it is extended to accommodate other cryptocurrencies than only Bitcoin. Complex transaction behavior analysis may be made more accurate by including sophisticated deep learning models like LSTM or GNN. Reporting of illicit activity might be automated through cooperation with law enforcement APIs and compliance tools. Over time, model predictions can be improved with the aid of a user feedback system. Additionally, adding mobile accessibility and sophisticated visualization dashboards would improve the system's usability and efficacy for more extensive anti-money laundering enforcement applications.

REFERENCES

[1] Ferretti, S., D'Angelo, G., & Ghini, V. (2025). Enhancing anti-money laundering frameworks: An application of graph neural networks in cryptocurrency transaction classification. IEEE Access.

[2] Radhan, A., Sumith, N., & Srividya, S. (2025, February). Exploring the Effectiveness of Machine Learning Models in Detecting Anomalous Transactions. In 2025 International Conference on Artificial Intelligence and Data Engineering (AIDE) (pp. 85-89). IEEE.

[3] Li, G., Mi, Y., Zhou, J., Zheng, X., & Wu, W. (2025). Group Based Detection of Cryptocurrency Laundering Using Multi-Persona Analysis. IEEE Transactions on Information Forensics and Security.

[4] Yu, Q., Xu, Z., & Ke, Z. (2024, November). Deep learning for cross-border transaction anomaly detection in anti-money laundering systems. In 2024 6th International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI) (pp. 244-248). IEEE.

[5] Irshad, F., Alkhalifah, T., Alturise, F., & Khan, Y. D. (2024). GCF-MLD: integrated approach for money laundering detection using machine learning and graph network analysis. IEEE Access.

[6] Wu, J., Liu, J., Zhao, Y., & Zheng, Z. (2021). Analysis of cryptocurrency transactions from a network perspective: An overview. *Journal of Network and Computer Applications, 190*, Article 103139. https://www.sciencedirect.com/science/article/pii/S1084804521001557

[7] Marasi, S., & Ferretti, S. (2024, January). Anti-money laundering in cryptocurrencies through graph neural networks: A comparative study. In *Proceedings of the IEEE 21st Consumer Communications & Networking Conference (CCNC)* (pp. 272–277).

[8] Rathore, M. M., Chaurasia, S., & Shukla, D. (2022, December). Mixers detection in Bitcoin network: A step towards detecting money laundering in crypto-currencies. In *Proceedings of the IEEE International Conference on Big Data (Big Data)* (pp. 5775–5782).

[9] Scharfman, J. (2022). Anti-money laundering compliance for cryptocurrencies. In *Cryptocurrency*

Compliance and Operations (pp. 91–114). Springer, Berlin, Germany.
[10] Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How blockchain can impact financial services—The overview, challenges and recommendations from expert interviewees. *Technological Forecasting and Social Change, 158*, Article 120166.
[11] Jullum, M., Løland, A., Huseby, R. B., Ånonsen, G., & Lorentzen, J. (2020). Detecting money laundering transactions with machine learning. *Journal of Money Laundering Control, 23*(1), 173–186.
[12] Gerbrands, P., Unger, B., Getzner, M., & Ferwerda, J. (2022). The effect of anti-money laundering policies: An empirical network analysis. *EPJ Data Science, 11*(1), Article 15.
[13] Serena, L., Ferretti, S., & D'Angelo, G. (2022). Cryptocurrencies activity as a complex network: Analysis of transactions graphs. *Peer-to-Peer Networking and Applications, 15*(2), 839–853.
[14] Pareja, A., Domeniconi, G., Chen, J., Ma, T., Suzumura, T., Kanezashi, H., Kaler, T., Schardl, T. B., & Leiserson, C. E. (2020, April). EvolveGCN: Evolving graph convolutional networks for dynamic graphs. In *Proceedings of the AAAI Conference on Artificial Intelligence*, *34*(4), 5363–5370.
[15] Lo, W. W., Kulatilleke, G. K., Sarhan, M., Layeghy, S., & Portmann, M. (2023). Inspection-L: Self-supervised GNN node embeddings for money laundering detection in Bitcoin. *Applied Intelligence, 53*(16), 19406–19417.
[16] Adewumi, A. O., & Akinyelu, A. A. (2017). A survey of machine-learning and nature-inspired based credit card fraud detection techniques. *International Journal of System Assurance Engineering and Management, 8*(2), 937–953.
[17] Popat, R. R., & Chaudhary, J. (2018, May). A survey on credit card fraud detection using machine learning. In *Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 1120–1125).
[18] Sinayobye, J. O., Kiwanuka, F., & Kyanda, S. K. (2018, May). A state-of-the-art review of machine learning techniques for fraud detection research. In *Proceedings of the IEEE/ACM Symposium on Software Engineering in Africa (SEiA)* (pp. 11–19).
[19] Mekterović, I., Brkić, L., & Baranović, M. (2018). A systematic review of data mining approaches to credit card fraud detection. *WSEAS Transactions on Business and Economics, 15*, 437–444.
[20] Sadgali, I., Sael, N., & Benabbou, F. (2018). Detection of credit card fraud: State of art. *International Journal of Computer Science and Network Security, 18*(11), 76–83.
[21] Patil, V., & Lilhore, U. K. (2018). A survey on different data mining & machine learning methods for credit card fraud detection. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3*(5), 320–325.
[22] Canillas, R., Talbi, R., Bouchenak, S., Hasan, O., Brunie, L., & Sarrat, L. (2018, December). Exploratory study of privacy preserving fraud detection. In *Proceedings of the 19th International Middleware Conference Industry* (pp. 25–31). https://doi.org/10.1145/3284028.3284032
[23] Zhou, X., Zhang, Z., Wang, L., & Wang, P. (2019, July). A model based on Siamese neural network for online transaction fraud detection. In *Proceedings of the International Joint Conference on Neural Networks (IJCNN)* (pp. 1–7). https://doi.org/10.1109/IJCNN.2019.8852295
[24] Zhang, Z., Zhou, X., Zhang, X., Wang, L., & Wang, P. (2018). A model based on convolutional neural network for online transaction fraud detection. *Security and Communication Networks, 2018*, Article 5680264. https://doi.org/10.1155/2018/5680264
[25] Zheng, L., Liu, G., Yan, C., Jiang, C., Zhou, M., & Li, M. (2020). Improved TrAdaBoost and its application to transaction fraud detection. *IEEE Transactions on Computational Social Systems, 7*(5), 1304–1316.
[26] Wang, Y., Adams, S., Beling, P., Greenspan, S., Rajagopalan, S., Velez-Rojas, M., Mankovski, S., Boker, S., & Brown, D. (2018, August). Privacy preserving distributed deep learning and its application in credit card fraud detection. In *Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)* (pp. 1070–1078).
[27] Tong, G., & Shen, J. (2023). Financial transaction fraud detector based on imbalance learning and graph neural network. *Applied Soft Computing, 149*, Article 110984.
https://www.sciencedirect.com/science/article/pii/S1568494623010025
[28] Dou, Y., Liu, Z., Sun, L., Deng, Y., Peng, H., & Yu, P. S. (2020, October). Enhancing graph neural network-based fraud detectors against camouflaged fraudsters. In *Proceedings of the 29th ACM International Conference on Information and Knowledge Management* (pp. 315–324). https://doi.org/10.1145/3340531.3411903
[29] Huang, X., Yang, Y., Wang, Y., Wang, C., Zhang, Z., Xu, J., Chen, L., & Vazirgiannis, M. (2022). DGraph: A large-scale financial dataset for graph anomaly detection. In *Proceedings of the 36th International Conference on Neural Information Processing Systems (NeurIPS)* (Vol. 35, pp. 22765–

22777). https://proceedings.neurips.cc/paper_files/paper/2022/file/8f1918f71972789db39ec0d85bb31110-Paper-Datasets_and_Benchmarks.pdf
[30] Defferrard, M., Bresson, X., & Vandergheynst, P. (2016). Convolutional neural networks on graphs with fast localized spectral filtering. In *Proceedings of Advances in Neural Information Processing Systems (NeurIPS)* (Vol. 29, pp. 1–9).

Author Profiles

Ranapratap Pola is currently an M.Tech student at Bonam Venkata Chalamayya Engineering College, pursuing a Master's degree in Computer Science and Engineering, He is Passionate about Machine Learning and Artificial Intelligence. He is proficient in C, C++, CNC Coding, and Python. His current research work focuses on a Machine Learning in Money Laundering Detection.

B. Ganga Bhavani is Research Scholar at Koneru Lakshmaiah Education Foundation (KLEF) Green Fields, Vaddeswaram and Asso- ciate Professor at Bonam Venkata Chalamayya Engineering College, Odalarevu. She holds an M.Tech degree in Computer Science and Engineering from GIET College, Rajahmundry. Her research areas are Machine Learning, Deep Learning and Artificial Intelligence. She has a number of patents related to ma- chine learning field and industrial designs on her innovative ideas and has been awarded with international patents and published dif- ferent articles in international conferences. She can be contacted at: Koneru Lakshma- iah Education Foundation (KLEF) Green Fields, Vaddeswaram, A.P – 522302. Email: bgangabhavani.bvce@bvcgroup.in. ORCID: https://orcid.org/0000-0003-1433-5832