RESEARCH ARTICLE OPEN ACCESS

Detection of Investment Scam-Related Bitcoin Addresses Via CatBoost Machine Learning Model

Nishant Tripathi
Dept. of Computer Science and Engineering, JAIN (Deemed-To-Be University), Bengaluru, Karnataka, India
nishant.tripathi@jainuniversity.ac.in

--************************----------------------------------

Abstract:

Bitcoin, one of the most well-known and widely used cryptocurrency, has grown in popular-ity over the years. Its decentralized nature, security and transparency has attracted all kinds of users. Bitcoin has been associated with various kinds of malicious activities such as in-vestment scams, money laundering, ransom, Darknet marketplace purchases etc. Investment scams like High Yield Investment programs have become a serious issue as new Investors who are not aware of this fall prey for these scams. They entice countless investors through promises of unrealistic returns on investments. The proposed research performs various Machine learning algorithms to determine which algorithm detects HYIP related bitcoin addresses more accurately. Testing reveals the CatBoost algorithm achieves 96% accuracy in detecting HYIP-related addresses.

Keywords — **Bitcoin , Machine Learning, High Yield Investment Program, Transaction retrieval.**

---------------------------------------************************----------------------------------

I. INTRODUCTION

Bitcoin acts as a decentralized and pseudonymous network which allows users to transact with each other directly without the need for intermediaries like banks. An Investment Program (HYIP) is an online illegal financial scheme that promises participants extraordinarily high returns on the deposits. These schemes pay existing investors using the funds from newcomers, creating a cycle that continues until the money runs out, leading to the collapse of the operation. Often referred to as "Ponzi schemes" after the infamous Charles Ponzi in the 1920s, these fraudulent programs have existed for over a century.

Consider perpetrator A approaches investor B with an existing offer of about an investment program offering 5% daily returns in bitcoin. A also mentions this scheme as a referral program which rewards users for bringing more people in the program. B will invest in this scheme and promote it to others and get extra re-ward for promoting it and B will get his returns regularly until no more investor will participate in the scheme and the program will collapse leaving B with no money and A will be running away. As this scheme does not generate any profits it just gives new investors money to the old investors and as new investors stop coming that scheme collapse leaving investors with no money and Bitcoin is the perfect platform for this scam as it has irreversible transactions and pseudo-anonymity make it an ideal tool for scammers. HYIP operators attract investors on cryptocurrency platforms like bitcoin talk and pages on reddit dedicated to bitcoin. Scammers post about their "investment opportunities" in relevant threads or create new ones to lure users interested in high-yield revenues. They also promote HYIPs aggressively on platforms like Facebook, Twitter, Instagram, Telegram, and Discord. People who are new in cryptocurrency fall for this marketing and become its prey.

To better understand this form of online criminal activity, we have dedicated significant time to gathering data from various HYIP websites and aggregator platforms. This research aims to focus on the scale and behaviour of HYIPs, to understand the behavioural dynamics and contribute to improving the financial landscape [13]. Most previous studies have conducted comparative analyses of widely used non-parametric machine learning models, particularly DT and RF models, to evaluate their classification accuracy on various datasets.

In this aspect, the proposed study aims to improve the detection of illegal users in bitcoin network by using a supervised learning approach. This involves gathering and analyzing the features that can classify the various types of illegal users for improving the accuracy and reliability to identify illegal actions within the bitcoin network. This contributes to more efficient monitoring and regulatory measures in the domain of cryptocurrencies [11],[6],[16]. The proposed study uses RF and XGB to evaluate the behavioural Dataset of bitcoin addresses. This dataset is well suitable for understanding user behaviours within the bitcoin eco-system, making it easier to distinguish between illegal and legal activities. To test the dataset, five well-known ML models, including DT , RF, XGB, KNN algorithm, and MLP algorithm.[19][16] After the experimentation, performance of each model is calculated with Accuracy, F1-Score, Recall, and Precision. The results in the study indicate that XGB is in the lead with RF followed by DT, MLP and KNN. This marks the effectiveness of XB and RF in handling the dataset accurately.[6],[11],[10]. The results also indicate that more effective monitoring and regulatory measures are needed in this rapidly growing realm of cryptocurrencies.

A. *Motivation and key contributions*

Bitcoin has been adopted by many users around the world due to its decentral-ized nature, security and simple transactions. However these same advantages are being exploited by Malicious users. Bitcoin has become one of the target to run fraudulent activities such as ponzi scheme, Ransom payments , Darknet market-place and High-Yield Investment programs and other illicit financial schemes. Identifying these fraudulent Bitcoin addresses becomes essential as they lure gullible and innocent users into their schemes.To identify such bitcoin addresses many existing studies have implemented supervised Machine learning(ML) algo-rithm on a labelled dataset which have made a significant progress to identify these Bitcoin addresses but there is still room for improvement. The proposed study addresses these limitations by doing an extensive literature survey for da-taset collection with labels , retrieving Bitcoin transaction data, Extracting Fea-tures and evaluating multiple ML models to identify the most accurate approach. The study Includes implementation of 9 different ML models that were men-tioned in the previous studies. Additionally, an ensemble model combining LightGBM, Gradient Boosting and CatBoost were performed to improve the Per-formance of the modeL. Among all the tested models, CatBoost showed the most accurate results as it had a perfect balance of F1-Score, Recall and Precision and after hyper tuning the classifier further enhanced its capabilities. It shows how important gradient boosting is to identify bitcoin addresses accurately.

II. LITERATURE SURVEY

Detecting whether a bitcoin address is illicit or not, has been an active area of study. Several studies have explored different machine learning approaches. They have also identified a proper category rather than just identifying licit or illicit bitcoin addresses such as identifying bitcoin addresses related to mixing services, ponzi schemes, Money laundering and HYIPs.

Shayegan et. al. (2022) proposed an anomaly detection tec hnique using trimmed_ KMeans algorithm,Showing advantage over traditional K Means. Their approach detected a number of theft cases, It highlights the effectiveness of the anomaly detection[3].similarly, Toyoda et al(2018) introduced a multi-class ser-vice to identify the class using transaction history achieving accuracy up to 72% using an owner-based scheme[2]. Lihao Nan and Dacheng Tao(2018) utilized Autoencoders to detect Bitcoin mixing services, it exceeds heuristic methods[1]. Wu et al.(2019) introduced the Forensic Analysis of Bitcoin Transaction (FABT) framework for identifying suspicious Bitcoin addresses, particularly forensic investigation like the Mt.Gox case[4]. Toyoda et al(2017) specifically targeted HYIP- related addresses by analysing frequency-based patterns. They achieved 83% accuracy which was a significant improvement in HYIP detection. In 2019 Toyoda et al. extended this work by introducing a larger dataset and achieving higher accuracy of 93.75%[7].

There are many studies to identify illicit bitcoin addresses by using KNN algorithm[6], Ensemble decision tree with 91% accuracy [9]. Additionally, studies which have used unsupervised ML algorithms to identify Ponzi related bitcoin addresses with 96% accuracy [10].Pham and lee (2016) used unsupervised learn-ing for anomaly detection and classifying suspicious activities within transactional graph [17].

Overall, the existing studies show that ML models applied to bitcoin fraud detection typically achieve accuracy rates between 80% to 95%, depending on the dataset. The proposed study integrates a well-labelled dataset and applies multiple ML models to identify HYIP-related Bitcoin addresses.

III. BACKGROUND

B. HYIP

HYIP is a type of financial fraudulent scheme that promises extraordinarily high returns within a short period. In reality, most HYIPs operate as Ponzi schemes, where returns to earlier participants are paid using the funds from newer participants rather than from legal business activities. These schemes rely on continuous recruitment of new participants to sustain payouts, and once the flow of new funding slows down, the operators disappear with the remaining funds, leaving investors at a loss.

How HYIPs Work

1. **Attraction & Promotion** – HYIPs advertise on social media, websites, and forums, claiming unrealistic daily or weekly returns (e.g., “Earn 5% per day with no risk!”).
2. **Initial Payouts to Build Trust** – Early investors receive payments to create credibility and encourage further investments.
3. **Rapid Growth** – More investors join, believing in the legitimacy of the program, while operators secretly siphon off funds.
4. **Collapse & Exit Scam** – The scheme collapses when new investments slow down, and the operators disappear, leaving investors with losses.

Since HYIPs exploit the anonymity of cryptocurrencies like Bitcoin, tracking and recovering lost funds is extremely difficult. This makes detecting HYIP-related Bitcoin addresses essential for preventing fraud and adding security in the crypto ecosystem.

How HYIP is Advertised

HYIPs depend on aggressive and false advertising strategies to gain attention of their investors and sustain their illegal activities. Most common method is creating a professional and legitimate looking website that promises to return unrealistic funds by showing manipulated financial reports, fake testimonials and countdown timers to create urgency. There are dedicated websites to advertise HYIPs as presented in figure 1.

Social media such as Instagram, Facebook, Twitter and Telegram play an im-portant role in promotions for HYIP. Operators make use of viral marketing tech-niques, paid promotions and influencers to advertise their unrealistic success stories, making it appear legitimate.

Youtube also plays a major role where HYIP organizers make video advertise-ments to show the fake earnings, proofs of withdrawals and falsified testimonies to trap investors. Referrals and associate programs encourage participants to trap new investors in exchange for rewards, turning them into unpaid promoters of the HYIP-related scam. HYIPs also make paid advertisements on digital currency forums, blogs, and websites. Some of these sites also ask to rank these schemes based on the activity of investors. These paid advertisements make such schemes appear legitimate. Scammers use spam campaigns to send promotional messages and mails with false claims of financial independence from fake investors. Tele-gram and Whatsapp are also some of the popular hubs for HYIP-related promo-tions. Scammers also target existing HYIP scheme participants to advertise on Ponzi-related forums and communities.

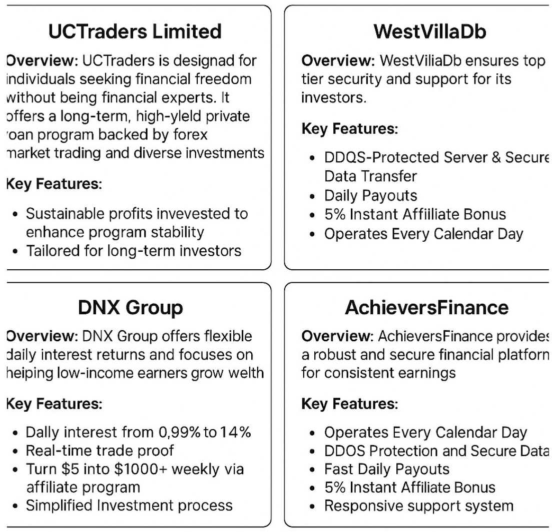

Fig. 1 Advertisement of HYIP on hyipexplorer.com

Since these individuals are already familiar with high-risk investment schemes, they are more likely to reinvest in similar programs, unknowingly perpetuating the scam. By leveraging these deceptive advertising strategies, HYIPs attract a continuous inflow of new participants, allowing the operators to siphon funds before eventually shutting down the scheme. Recognizing these tactics is crucial in preventing financial losses and identifying fraudulent activities in the crypto-currency space.

C. Dataset availability and selection

To detect HYIP-related Bitcoin addresses depends on the availability of labelled dataset. One of the main challenges was to find a well-labeled dataset. To over-come this challenge a survey was conducted to identify suitable dataset of this study that are publicly available.

A survey of 23 papers was conducted to determine if they have a dataset availa-ble or not. By analyzing methodologies. It was determined 7 of the studies have publicly available dataset, 5 studies have not disclosed the dataset they have worked on. 3 have used existing Datasets available on the internet and 8 studies have the dataset private.

TABLE I
DATASET AVAILABILITY

S. No.	Study Title	Dataset Availability
1	Double and Nothing: An Exploratory Study on Cryptocurrency Giveaway Scams	Publicly Available
2	Assessment of Bitcoin Address Classification Using Transaction History Features	Publicly Available
3	Multi-Class Service Detection in Bitcoin Using Transaction Summarization Techniques	Publicly Available
4	Analysis of Illicit Behavioral Patterns of Bitcoin Users in Criminal Transactions	Publicly Available
5	Identification of Malicious Bitcoin Entities via Supervised Ensemble Learning Models	Publicly Available
6	Tracing Illicit Financial Transfers: A Case Study on Bitcoin Laundering Across Digital Services	Not Available
7	The Postmodern Ponzi Scheme: A Data-Driven Study of High-Yield Cryptocurrency Investment Frauds	Not Available

IV. IMPLEMENTATION

D. Architecture

The proposed research involves Bitcoin dataset[2] is normalized and balanced for feature extraction and ML algorithm application as presented in Figure 2.

A labelled dataset was selected which includes 26,314 bitcoin addresses sourced from "Multi-Class Bitcoin-Enabled Service Identification Based on Transaction History Summarization."[2]. The dataset is well structured and has several Categories including: HYIP, Pools, Gambling, Mixers, Market, Exchange and Faucet. Transaction retrieval process was done on 26,314 bitcoin addresses to retrieve transaction history of those Bitcoin addresses using Blockchain.com API. A sample data represented as Data=$\{(x_1, y_1), (x_2, y_2), \ldots\ldots\ldots, (x_i, y_i)\}$, where i denotes number of samples, x_i is feature vector and $y_i$is labels as in equation (1)

$$Data = \{(x_i, y_i)\}^N{}_{i=1}, x_i \in R^d , y_i \in \{0,1\} \ldots\ldots (1)$$

y_i is a label where 0 is non HYIP and 1 is HYIP. N is the number of addresses . d is a number of features.

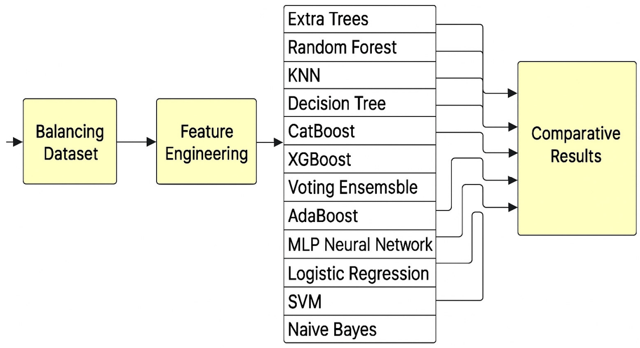

Fig 2. Model Structure

E. FEATURE Extraction

After transaction retrieval, features are extracted from the transaction data retrieved presented in Table.2. The transaction attributes of each Bitcoin address are set of features.

The feature extraction function F takes preprocessed data $x'_i \in R^{d'}$ and transforms it into new vector $z_i \in R^k$ with only k features.

$$z_i = F(x'_i), \text{ where } z_i \in R^k \text{ ....(2)}$$

z_i are new feature vector and (x'_i) is preprocessed data as shown in equation (2).

Feature	Explanation
Freq T	Indicates how frequently a Bitcoin address is used, calculated as the total number of transactions made per day.
rx_ tx_ ratio	Represents the proportion of incoming transactions relative to the total number of transactions.
rx_ tx_ coin base	Denotes the fraction of transactions originating from coin base rewards.
rx_ payback	A measure of self-loop transactions, calculated by the ratio of addresses appearing in both input and output fields.
mean_ inputs spent	The average number of input addresses used per outgoing transaction.
mean_ outputs spent	The average number of output addresses utilized per outgoing transaction.
rx_ sent	Proportion of outgoing transactions relative to the total number of all transactions linked to the address.
Total_ cluster_ size	Reflects the overall transaction volume linked to a particular address cluster.
Sending amount	The cumulative amount sent from the address to others over all transactions.
Receiving amount	The total amount received by the address across all incoming transfers.
Balance	The final amount of Bitcoin remaining in the address after all transactions are processed.

In detecting High-Yield Investment Programs (HYIPs) using Bitcoin addresses, certain features are particularly telling. High transaction frequency (FreqT) and large transaction volumes (Total_cluster_size) can indicate active, potentially deceptive operations. A high ratio of received transactions (rx_tx_ratio) and total receiving amount may suggest the address is collecting substantial investments. Conversely, a high ratio of sent transactions (rx_sent) and sending amount could point to distributing returns or payouts. Features like the payback ratio (rx_payback) and the mean number of inputs/outputs (mean_inputs_spent and mean_ouputs_spent*)* reveal patterns of fund aggregation and distribution, typical of HYIPs. balances and transaction patterns further support the identification of such schemes. In the Proposed work, each feature is calculated based on nTx ((Number of substantial transactions) = 100 for each address or owner. This approach is designed to minimize computational time while maintaining classification accuracy. By focusing on a limited number of recent transactions, the methodology efficiently captures relevant behavioral patterns without compromising the quality of the classification results.

F. Algorithm application

In this study, several ml algorithms were applied to classify Bitcoin addresses and detect HYIP-related activity. Each algorithm was evaluated based on its performance in identifying Class 1.

Let M_j be the machine learning model j being different models like Naive Bayes, MLP, KNN, Extra trees etc.

$z_i \in R^k$ the feature vector of i th sample $\hat{y}_i^{(j)}$ is the prediction of model M_j .

$$\hat{y}_i^{(j)} = M_j(Z_i) \text{ ......(3)}$$

Each M_j is trained using loss function . A loss function tells the model how wrong it is and it needs to be minimized during training as shown in equation (3).

TABLE 2
RESULTS OF MACHINE LEARNING MODELS

MODEL	ACCURACY	PRECISION (HYIP)	RECALL (HYIP)	F1 (HYIP)
ET	0.968	0.88	0.63	0.74
R F	0.97	0.89	0.62	0.73
KNN	0.956	0.74	0.59	0.66
DT	0.948	0.62	0.67	0.64
CatBoost	0.96	0.66	0.80	0.72
XGB	0.93	0.49	0.85	0.62
Voting Ensemble	0.93	0.52	0.83	0.64
AdaBoost	0.954	0.86	0.43	0.57
MLP	0.944	0.86	0.26	0.40
LR	0.929	0.50	0.03	0.06
SVM	0.929	0.00	0.00	0.00
NB	0.208	0.08	0.96	0.15

This systematic evaluation of machine learning algorithms shown in TABLE 2 helped identify the most effective models for producing accurate results in the study, guiding the final selection of the effective algorithm for further analysis and implementation. The classifiers have been tested performance has been evaluated . The following 3 classifiers have been choosen:

- Random Forest
- LightGBM+XGB(Voting ensemble)
- CatBoost

The performance of the classifiers in detecting HYIP transactions was evaluated based on PRECISION, F1-SCORE, and RECALL, particularly for the minority class of HYIP transactions. Here is a detailed breakdown of how each classifier performed:

1. Random Forest Classifier: While the Random Forest Classifier shows high overall accuracy, its performance in detecting HYIP transactions (the minority class) was less impressive. The high precision of 0.89 means that when the Classifier predicted an address as a HYIP, it was correct most of the time. However, the recall of 0.62 indicates that it missed a significant number of actual HYIP addresses. The F1-Score of 0.73 shows a moderate balance between recall and precision, but overall, Random Forest struggles to detect HYIP transactions reliably, making it Ineffective for handling the minority class[8].

2. LightGBM + XGBoost Classifiers: This ensemble approach, combining LightGBM and XGBoost, performed slightly worse in terms of overall accuracy at 93%. However, for the detection of HYIP transactions, the recall was much higher at 0.83, meaning it identified more of the actual HYIP addresses compared to Random Forest. Precision was lower at 0.52, indicating that it produced more false positives (incorrectly labeling non-HYIP as HYIP). The F1-score of 0.64 reflects a better performance in detecting HYIP class compared to RF, though the trade-off was a reduced overall precision. This classifier is better suited for capturing more HYIP cases but struggles with misclassifications[8].

3. CatBoost Classifiers: CatBoost achieved an overall accuracy of 96%,with FPR of 3.18% and TPR of 96.34% matching Random Forest in this regard. However, its performance in detecting HYIP transactions was stronger, with a Precision of 0.66 and a Recall of 0.80. This balance between Precision and Recall resulted in an F1-Score of 0.72, indicating that CatBoost performs well across the board for both precision and recall. It strikes a better balance compared to both Random Forest and the LightGBM + XGBoost ensemble, making it the most effective classifier for detecting the minority class of HYIP transactions without sacrificing too much in overall accuracy or generating excessive false positives.

G. Performance Evaluation

Random Forest is strong in terms of precision, meaning it's very good at identify-ing actual HYIP cases correctly. However, its recall is lower, meaning it misses a significant number of true HYIP cases. While the overall accuracy is good, it sacrifices catching all possible HYIPs, which might not be ideal if you're aiming for comprehensive detection. LightGBM and XGB models catch more HYIP-related cases than RF, as they are seen to perform in recall. However, the lower precision creates a boundary as it indicates false positives, meaning cases are flagged as HYIP that aren't. This situ-ation makes them efficient in finding more HYIP cases but can be less precise overall. They can be used when missing a HYIP is more important than having a few positives. However, CatBoost provides the optimal balance between Precision, F1-Score and Recall. It maintains accuracy, making it reliable for detecting HYIP transactions. CatBoost doesn't produce as many false positives as Voting ensemble and RF model. This balance makes it the most suitable choice for handling the minority class of HYIP cases without any compromise in detection.

V. CONCLUSION

In conclusion, the study proposes an approach to exchange the detection of HYIP-related bitcoin addresses by using a wide variety of features such as trans-action frequency, transaction volume, inflow ratio, outflow ratio, cluster size etc. The proposed model CatBoost was found best to detect HYIP-related addresses having a balance both precision and recall effectively. The selected model has accuracy 96% with FPR of 3.18% and TPR of 96.34%. The study shows the im-portance of diverse features and ml algorithms.

REFERENCES

[1] Nan, L., Tao, D.: Bitcoin mixing detection using deep autoencoder. In: 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), pp. 280–287. IEEE, Guangzhou (2018). https://doi.org/10.1109/DSC.2018.00047

[2] Toyoda, K., Ohtsuki, T., Mathiopoulos, P.T.: Multi-class bitcoin-enabled service identification based on transaction history summarization. In: *2018 IEEE Int. Conf. on Internet of Things (iThings), GreenCom, CPSCom, and SmartData*, pp. 1153–1160. IEEE (2018)

[3] Fard, M.S., Sabor, H., Uddin, M., Chen, C.L.: A collective anomaly detection technique to detect crypto wallet frauds on the Bitcoin network. *Symmetry* **14**, 328 (2022). https://doi.org/10.3390/sym14020328

[4] Wu, Y., Luo, A., Xu, D.: Forensic analysis of bitcoin transactions. In: *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 167–169. IEEE (2019)

[5] Toyoda, K., Ohtsuki, T., Mathiopoulos, P.T.: Identification of high yielding investment programs in Bitcoin via transactions pattern analysis. In: *GLOBECOM 2017 - IEEE Global Communications Conference*, pp. 1–6. IEEE, Singapore (2017). https://doi.org/10.1109/GLOCOM.2017.8254420

[6] Gao, M., Lin, S., Tian, X., He, X., He, K., Chen, S.: A bitcoin service community classification method based on Random Forest and an improved KNN algorithm. *IET Blockchain* **4**, (2024). https://doi.org/10.1049/blc2.12064

[7] Toyoda, K., Mathiopoulos, P.T., Ohtsuki, T.: A novel methodology for HYIP operators' bitcoin addresses identification. *IEEE Access* **7**, 74835–74848 (2019). https://doi.org/10.1109/ACCESS.2019.2921087

[8] Lin, Y.J., Wu, P.W., Hsu, C.H., Tu, I.P., Liao, S.W.: An evaluation of bitcoin address classification based on transaction history summarization. In: *2019 IEEE International Conference on Blockchain*, pp. 302–310. IEEE (2019). https://doi.org/10.1109/BLOC.2019.8751410

[9] Nerurkar, P., Bhirud, S., Patel, D., Ludinard, R., Busnel, Y., Kumari, S.: Supervised learning model for identifying illegal activities in Bitcoin. *Applied Intelligence* **51**, 3824–3843 (2021)

[10] Bartoletti, M., Pes, B., Serusi, S.: Data mining for detecting bitcoin Ponzi schemes. In: *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 75–84. IEEE, Zug (2018). https://doi.org/10.1109/CVCBT.2018.00014

[11] Nerurkar, P., Busnel, Y., Ludinard, R., Shah, K., Bhirud, S., Patel, D.: Detecting illicit entities in bitcoin using supervised learning of ensemble decision trees. In: *Proc. 10th Int. Conf. on Information Communication and Management*, pp. 25–30 (2020)

[12] Moore, T., Han, J., Clayton, R.: The postmodern Ponzi scheme: empirical analysis of high-yield investment programs. In: *Financial Cryptography and Data Security: 16th Int. Conf., FC 2012, Revised Selected Papers*, pp. 41–56. Springer, Berlin (2012)

[13] Li, X., Yepuri, A., Nikiforakis, N.: Double and nothing: Understanding and detecting cryptocurrency giveaway scams. In: *NDSS Symposium 2023* (2023). https://doi.org/10.14722/ndss.2023.24584

[14] Fanusie, Y., Robinson, T.: Bitcoin laundering: An analysis of illicit flows into digital currency services. Center on Sanctions & Illicit Finance, Washington DC (2018)

[15] Xiang, Y., Li, Y., Hu, H., Liu, L., Zhou, W., Zhang, Y.: BABD: A bitcoin address behavior dataset for pattern analysis. *IEEE Transactions on Information Forensics and Security* **19**, 2171–2185 (2024). https://doi.org/10.1109/TIFS.2023.3347894

[16] Pham, T., Lee, S.: Anomaly detection in bitcoin network using unsupervised learning methods. *arXiv preprint* arXiv:1611.03941 (2016)

[17] Bynagari, N.B., Ahmed, A.A.: Anti-money laundering recognition through the gradient boosting classifier. *Academy of Accounting and Financial Studies Journal* **25**(5), 1–11 (2021)

[18] Ibrahim, R.F., Elian, A.M., Ababneh, M.: Illicit account detection in the Ethereum blockchain using machine learning. In: *2021 International Conference on Information Technology (ICIT)*, pp. 488–493. IEEE, Amman (2021). https://doi.org/10.1109/ICIT52682.2021.9491653

[19] Kondor, D., Pósfai, M., Csabai, I., Vattay, G.: Do the rich get richer? An empirical analysis of the Bitcoin transaction network. *PLoS ONE* **9**(2), e86197 (2014). https://doi.org/10.1371/journal.pone.0086197

[20] Tripathi, N. ., Singh, C. ., & Sharma, K. K. . (2024). Optimizing Network Efficiency and Stability through Increased Sectorization Enhanced Protocol (ISEP) in Wireless Networks. International Journal of Intelligent Systems and Applications in Engineering, 12(15s), 08–16. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/4703

[21] Tripathi, N. ., Singh, C. ., & Sharma, K. K. . (2023). Enhancement of Performance Metrics of Heterogeneous Wireless Camera Sensor Network with Functionalization of Extensive Zonal Stable Election Protocol using Threshold Amplification and Residual Energy. International Journal on Recent and Innovation Trends in Computing and Communication, 11(8s), 657–669. https://doi.org/10.17762/ijritcc.v11i8s.7253

[22] N. Tripathi and K. K. Sharma, "Analytical Review of Different Routing Methodologies and Clustering Techniques in WSN/WCSN leading to Cooperative Communication," 2020 IEEE International Conference for Innovation in Technology (INOCON), Bangluru, India, 2020, pp. 1-6, https://doi.org/10.1109/INOCON50539.2020.9298208

[23] Tripathi, N., Sharma, K.K. (2022). Distributed and Hierarchical Clustering Techniques Comparison in Wireless Camera Sensor Networks. In: Kaiser, M.S., Bandyopadhyay, A., Ray, K., Singh, R., Nagar, V. (eds) Proceedings of Trends in Electronics and Health Informatics. Lecture Notes in Networks and Systems, vol 376. Springer, Singapore. https://doi.org/10.1007/978-981-16-8826-3_33

[24] Nishant Tripathi, Charanjeet Singh, Kamal Kumar Sharma, Praveen Kumar "Load Balancing Strategies in Wireless Camera Sensor Networks: Implementation, Complexity, and Applications" is published

in AIP Conference Proceedings for 1st International Conference on Recent Advancements in Computing Technologies & Engineering. https://doi.org/10.1063/5.0217184

[25] Lorenz, J., Silva, M.I., Aparício, D., Ascensão, J.T., Bizarro, P.: Machine learning methods to detect money laundering in the bitcoin blockchain in the presence of label scarcity. In: *Proceedings of the First ACM International Conference on AI in Finance*, pp. 1–8 (2020)

[26] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008). https://bitcoin.org/bitcoin.pdf

[27] Samsudeen, Z., Perera, D., Fernando, M.: Behavioral analysis of bitcoin users on illegal transactions. *Advances in Science, Technology and Engineering Systems Journal* **4**(2), 402–412 (2019)