International Journal of Business, Management and Visuals (IJBMV), ISSN: 3006-2705
Volume 5, Issue 1, January-June, 2022, Available online at: https://ijbmv.com

Anomaly Detection in Financial Transactions using Machine Learning and Blockchain Technology

Vineet Dhanawat

Independent Researcher, USA

ABSTRACT

Propose: Digitally signed transactions are the cornerstone of data connected to repressive chains that are kept in distributed ledgers. In particular, cryptocurrency has grown to become a place of refuge for criminal financing operations. These illegal patterns may be found by machine learning. With the advent of machine learning (ML), the capabilities to identify and mitigate fraudulent activities have significantly improved. This paper extract outlines the application of ML techniques in detecting anomalous transactions, highlighting the methodologies, challenges, and future directions. Anomaly detection in financial transactions is a critical task for maintaining the integrity and security of financial systems.

Aim: The financial industry has always been susceptible to fraud, necessitating robust mechanisms for anomaly detection. Traditional methods, reliant on rule-based systems, struggle to adapt to the evolving nature of financial fraud. Machine learning offers a dynamic and efficient approach to detecting anomalies in transactions by learning from historical data, identifying patterns, and flagging transactions that deviate from these patterns.

Keywords: Machine Learning (ML), Accuracy, Cyber-Attack, Block Chain, Cryptocurrencies, Digital Environments

INTRODUCTION

Blockchain technology has become prevalent in various application sectors, such as financial technology, software development, transportation, and the Internet of Things (IoT). Specifically, distributed blockchain technology forms the foundation of digital currencies like Bitcoin and the Ethereum network, which maintain transaction records and ensure computational integrity through robust hashing. The fundamental structure of cryptocurrency networking, built on Peer-to-Peer (P2P) connections and possibly not shielded by computational encryption, presents a serious security flaw.

For instance, over P2P overlays [1], the distributed unanimity protocol, which powers Bitcoin, functions with little credibility and genuine support (such as unambiguous text). Earlier studies have successfully demonstrated numerous vulnerabilities of blockchain infrastructures to assaults, including Distributed Denial of Service (DDoS), Eclipse, spoofing, and Sybil attacks. [1, 2].

For a considerable time, anomaly detection has remained a prominent research focus for monitoring system health, serving as a supplementary defence mechanism. This capability is essential for promptly identifying malicious activity and implementing necessary measures. Unlike conventional rule-based detection, which relies on pre-established signatures and is limited to known attacks, anomaly detection can differentiate between authorized operations and previously unexplored attacks by discerning patterns of lawful activity [2, 3].

Given its significance, numerous studies have examined anomaly identification in Bitcoin and blockchain networking. However, these studies have primarily focused on the distributed ledger within specific application contexts (such as transactions) and targeted particular types of attacks (e.g., double-spending, de-anonymization) [4, 5].

In this study, we employ a novel strategy to pinpoint potential threats to blockchain network security, focusing on the assessment and analysis of blockchain network communication traces rather than ledger data. Furthermore, our approach deviates from conventional network anomaly detection techniques that rely on connection data. We are primarily interested in identifying whether harmful content is present in peer-to-peer traffic rather than determining whether a connection between two nodes is abnormal [5, 6]. This distinction is crucial as application data, such as broadcasting Bitcoin messages, can be transmitted between two nodes of the blockchain via what is known as an overlay link [6].

Rule-based systems play a crucial role in Anti-Money Laundering (AML) efforts within the banking industry. However, vulnerabilities arise due to the relatively low identification rates and high False-Positive Rates (FPR) associated with publicly available rule sets. By extracting intricate patterns from historical data, Machine Learning (ML) methods can overcome the limitations of rule-based systems and have the potential to reduce FPRs while

increasing detection rates. Recently, a dataset comprising 200 thousand labelled transactions using Bitcoin was published, and it was utilized to evaluate various unsupervised networks.

Unfortunately, institutions often lack large-scale labelled datasets, making supervised approaches impractical. There are two main reasons for this labelling scarcity. Firstly, it's unlikely that all or even the majority of money laundering groups can be identified due to the continuously growing complexity of these schemes. Secondly, manual annotation is costly, and labels from law enforcement agency investigations take time to materialize [7, 8]. Therefore, techniques that require no labels (unsupervised learning) or only a few variables (active learning) are crucial for accurately assessing the practical feasibility of Machine Learning for Anti-Money Laundering (AML) purposes [9].

The complexity of the digital signing process is closely tied to most usability issues associated with digital signatures. In the realm of blockchain innovation, users' digital assets may be less secure because they can only transfer digital assets through properly executed and digitally signed transactions [10, 11]. Whenever a user intends to transfer an online property, they must provide a digitally signed transaction, a process that can only be completed within the aforementioned intricate digital signing procedure. If the digital signature process is conducted hastily, especially in the case of multiple transfers over an extended period, the confidentiality of electronic files may be compromised [11, 12].

Potentially hostile competitors may exploit this user activity and attempt to persuade them to sign transactions that could harm their digital assets. For instance, when a user conducts a transaction, transferring a specific amount of bitcoin via a web application (a decentralized application), the web application establishes and presents the transaction details to the user to facilitate the digital signature process [12]. Once digitally signed, the transaction is broadcast to the blockchain community and becomes irreversibly completed.

If the program generates a fraudulent transaction with tampered data — for example, specifying a larger quantity than what the user initially intended — a serious issue may arise. The user might unwittingly approve the fraudulent transaction, leading to irreversible consequences and financial loss. However, this work introduces a machine learning-based technique aimed at streamlining the digital signature process. To mitigate the risk of the aforementioned attack scenario [13, 14], the technique incorporates anomalous transaction detection alongside automatic electronic signatures.

The goal of this article is to introduce a revolutionary technique that enables automatic digital signing of transactions conducted via blockchain, thus alleviating the need for users to manually sign and review every transaction [15, 16]. The proposed approach offers an automated and personalized digital signature procedure for blockchain transactions. Additionally, it incorporates additional security measures, such as an anomaly detection system based on the user's personalized transaction data.

The designated transaction, involving the transfer of cryptocurrency from sender A to receiver B [17], is subsequently digitally signed on behalf of the sender by integrating the proposed method into blockchain-specific programs (e.g., wallets) for managing the digital authentication process. However, an exception is made for potentially anomalous transactions that could harm the sender. In such cases, manual consent from the sender is required before a transaction can be digitally signed. The characteristics of the suggested method also help overcome existing usability issues with digital signatures, which may inadvertently arise during use and hinder the widespread adoption of blockchain-based technology [18].

From a protocol architecture perspective, the immutability and irreversibility of the new ledger, Tangle, largely depend on cryptographic primitives such as hashing, permutations, etc., which are often probabilistic and contingent on the network conditions [19]. Therefore, ensuring integrity and confidentiality for interactions within the IOTA protocols is crucial. Traditional methods and techniques for enhancing IOTA security typically rely on explicit and statistical domain-based solutions, which are neither scalable nor compatible with a broader range of security threats.

Through the utilization of a reinforcement learning-based approach, we aim to detect and anticipate any security attacks targeting the Directed Acyclic Graph (DAG)--based endpoints and the graph itself, thereby addressing the existing gap in our work. Our method is grounded in the multiclass instructional technique known as Error-Correcting Output-Code. Notably, error-correction coding has long been employed in machine learning as a decentralized form of representation. Output coding serves as a solution to multiclass classification challenges. While existing output coding techniques have predominantly focused on classifying data using predetermined output codes, our implementation defines output codes for addressing issues about multiple classes.

We leverage the concept of ongoing codes in our solution, framing the task as a constrained optimization problem. Employing a mathematical technique akin to the window-sliding approach, we exploit the Tangle's dynamic growth along the time axis to extract features. This enables us to derive highly accurate indices using the information obtained from training samples.

Bitcoin is the most popular blockchain application, essentially constituting a form of digital currency created using cryptography. As of October of that year, it boasted a market valuation of approximately $359.7 billion. Globally, there were 7,378 cryptocurrencies in use, with Bitcoin commanding over 58.3% of this total. By leveraging blockchain technology to store transaction records, Bitcoin facilitates the creation, issuance, and exchange of currency while establishing a decentralized ledger shared among its users. For security and anonymity, Bitcoin employs anonymous identities, enabling instantaneous, low-cost international transactions. According to Blockchain.info, a real-time blockchain surveillance website, over 650,000 blocks have been produced, with an average of around $21 billion worth of transactions being recorded on the Bitcoin blockchain daily.

Due to Bitcoin's anonymity, low cost of instant transfers, and substantial economic value, it has been associated with numerous criminal activities. These illicit activities encompass a range of categories, including the use of ransomware, money laundering, theft, fraud, and transactions on dark web markets. Among these, Bitcoin theft stands out as one of the most detrimental.

Once the largest Bitcoin trading site in the world, Mt. Gox, revealed in February 2014 that 850,000 Bitcoins worth over $450 million may have been stolen before declaring bankruptcy. Similarly, in August of the same year, the Hong Kong-based market Bitfinex reported an attack on its security, resulting in the theft of $72 million worth of Bitcoins from user accounts. Following these events, Bitcoin's price dropped by 20%. The ability to identify Bitcoin theft events and promptly provide early warnings holds significant theoretical importance and practical relevance, as such events have a substantial impact on cryptocurrency security and even socio-economic stability.

The current body of research includes several studies on criminal activities involving Bitcoin and other public-chain electronic currencies. In a study conducted in 2016, the features of the Bitcoin user and transaction graphs were extracted using power law and densification law methodologies. Subsequently, three unsupervised methods—the Local Outlier Factor (LOF), One-Class Supported Vector Machine (OCSVM), and Mahalanobis Distance-Based Method (MDB)—were employed to identify thirty known Bitcoin events that were considered unusual [20].

In 2017, researchers examined the transaction history of the High Yield Investment Plan (HYIP) digital currency. They analyzed Bitcoin addresses and extracted characteristics of recognized transaction patterns. Using supervised learning, they successfully categorized over 1,500 Bitcoin addresses, achieving an 83% recall rate and a 4.4% False Positive Rate (FPR).

In 2018, a study focused on Bitcoin Ponzi schemes concluded. The researchers conducted a survival analysis to identify variables influencing the fraud's longevity. Through an examination of 1,424 posts on Bitcoin Talk, they identified 1,780 distinct Bitcoin Ponzi schemes. Their analysis revealed a positive association between the duration of interaction between scammers and victims and the scheme's sustainability.

In 2018, machine learning and data mining techniques were applied to identify Ponzi scams on Ethereum. Researchers found 45 Ethereum smart contracts that operated pyramid schemes by examining the contracts, extracting transaction capabilities and coding sound frequency characteristics from the contracts' accounts and opcodes, and utilizing eXtreme Gradient Boosting (XGBoost) to develop detection models. Additionally, they estimated the total number of Ponzi schemes on Ethereum to be above 400.

In 2019, researchers tested the new fraudulent behaviour Honeypot in Ethereum. Using Honeypot's taxonomy as a basis, they developed a method called HONEYBADGER that utilizes symbolic execution and heuristics to automatically detect Honeypot fraud.

Attack detection methods can be broadly categorized into three primary categories: misuse-based, hybrid-based, and anomaly-based classification. Misuse-based classification involves analyzing pre-recorded malicious activity signatures and is commonly used to identify known attacks. In this approach, minimizing false alarms or alerts caused by well-known attacks is crucial.

To make the strategy effective, some adjustments to the dataset signatures and attack standards are necessary. With the advancements in intelligent machines, researchers have been compelled to utilize decentralized Intrusion Detection Systems (IDSs) that integrate various Machine Learning (ML) techniques, including optimization algorithms, Deep Learning (DL), and Artificial Neural Networks (ANNs). However, the ability of ANNs to handle the intricate details of IDS systems is generally limited.

Based on the total number of layers in Artificial Neural Networks (ANNs), Deep Learning (DL) is a subgroup of Machine Learning (ML) that encompasses both supervised and unsupervised learning methodologies. Each layer consists of specific synapses whose functions are activated and utilized to generate non-linear outcomes. While inspired

by the biological architecture of brain neurons, this technique applies to general neural network data processing and transmission systems. DL algorithms employ a hierarchical multiple-level learning approach to extract essential abstract features from raw data.

This research introduces a blockchain-assisted heuristics-based algorithm that integrates machine learning-driven recognition and classification.

Objective of the Study

- Develop adaptable models to stay ahead of new risks in the financial ecosystem by continuously evolving and learning from emerging fraudulent behaviour patterns.
- Automate anomaly detection to optimize resource allocation within financial institutions, freeing up human resources to focus on more complex investigations and strategic initiatives.
- Establish performance metrics and benchmarks, including detection accuracy, false positive rates, response time, and scalability, to systematically evaluate the effectiveness of anomaly detection algorithms.

LITERATURE REVIEW

In the study conducted by Aziz (2022) [21], Ethereum is described as an online platform that utilizes blockchain technology to decentralize data by distributing copies of smart contract codes to thousands of users globally. Ethereum functions as an international digital currency, facilitating value transfer without requiring oversight or intervention from third parties. However, as e-commerce expands, the proliferation of illegal activities such as bribery, money laundering, and phishing poses a significant threat to trade security.

The article suggests employing the Light Gradient Boosting Machine (LGBM) approach to reliably identify fraudulent transactions on Ethereum. Additionally, the study examines various models, including Random Forest (RF) and Multilayer Perceptron (MLP), among others, based on machine learning and computational science techniques, to categorize Ethereum fraud detection datasets with limited features. Subsequently, the metrics of these models are compared with the LGBM technique. A comparison analysis of bagging model scores is provided to determine the suitability of the suggested methodology.

The results indicate that Extreme Gradient Boosting (XGBoost) and Light Gradient Boosting Machine (LGBM) algorithms achieve the highest accuracy figures, with LGBM demonstrating a higher accuracy rate of 98.60% for the given dataset scenarios. Furthermore, by employing hyper-parameter tuning to further optimize the LGBM, a precise result of 99.03% accuracy is attained.

In the study conducted by Elmougy (2021) [22], it is observed that the application of blockchain technology extends beyond the financial services and digital asset industries, with the technology steadily gaining momentum. The presence of a public ledger accessible to everyone makes it easy to verify the legitimacy of activities and accounts on blockchain technology. However, some malicious actors attempt to exploit Bitcoin owners, threatening the reliability of the blockchain.

The objective of this research is to identify fake accounts and transactions by detecting irregularities in the transaction networks of the two largest cryptocurrencies, Ethereum and Bitcoin. The study involves extracting information from over thirty billion transactions on the Bitcoin protocol and validating transactions from over 500 thousand accounts on the Ethereum network. GPU-accelerated machine learning algorithms, such as Support Vector Machine models, Random Forest, and Logistic Regression, are employed for this purpose. Through sensitivity analysis, the study offers insights into the significance of features and trains precise models that facilitate the adoption of techniques in automated systems for fraud identification.

In the study by Signorini (2020) [23], anomaly detection solutions, which play a crucial role in automatically identifying and filtering out unusual behaviours, are highlighted for safeguarding information systems and networks from unforeseen attacks. Over time, various strategies have been developed with the aim of reducing the false positive rate. Notably, no proposal has addressed attacks specifically targeting systems built on the blockchain. Therefore, the study introduces BAD: Blockchain Anomaly Detection, which is the first tool designed explicitly for detecting abnormalities in blockchain-based systems. BAD is a comprehensive framework that utilizes a variety of components and blockchain metadata at its core to identify potentially harmful behaviour.

In the study by Ofori-Boateng (2021) [24], a novel topological perspective is presented for identifying structural anomalies in dynamic multi-layered networks driven by the recent surge in illicit activities, including cross-cryptocurrency trading. The authors propose that anomalies stemming from multilayer abnormalities in the blockchain's

transaction graph may manifest as aberrant patterns within the network's shape attributes. To systematically monitor the network's development and identify modifications to its underlying geometry and topology, the authors utilize clique permanent homology on graphs. They introduce a layered, persistent diagram, a novel overview of multilayer networks, and demonstrate its stability against perturbations in input data. By validating their novel topological anomaly recognition paradigm on dynamically multilayer systems from the Ethereum Blockchain and the Ripple Credit Networks, the authors show that their stacked persistent diagram method significantly outperforms state-of-the-art approaches.

In the study by Bhowmik (2021) [25], the impact of fraudulent transactions on the economics and confidence of a blockchain network is discussed. While techniques like proof of work or proof of stake can confirm transaction genuineness, they cannot verify the characteristics of individuals transacting or verifying transactions, leaving blockchain networks vulnerable to fraud. The study proposes leveraging machine learning algorithms as a strategy to combat deception. Two types of machine learning approaches, supervised and unsupervised, are explored. The study focuses on verifying the authenticity of transactions and distinguishing between authentic and fraudulent ones using various supervised machine-learning algorithms. Additionally, the study provides a thorough analysis of several supervised artificial intelligence techniques, including multilayer perceptrons, logistic regression, decision tree modelling, Naive Bayes, and others, for the stated purpose.

METHODOLOGY

The machine learning approach for detecting attacks was presented in this paper. We present the research approach used in this study. The process began with gathering the dataset and performing the required preprocessing steps. The data was then split into two parts: one for training and the other for testing. Sampling techniques were applied solely to the training portion, leaving the testing dataset untouched. This sampled dataset was then used to train a range of machine learning models, both single and combined (ensemble) classifiers.

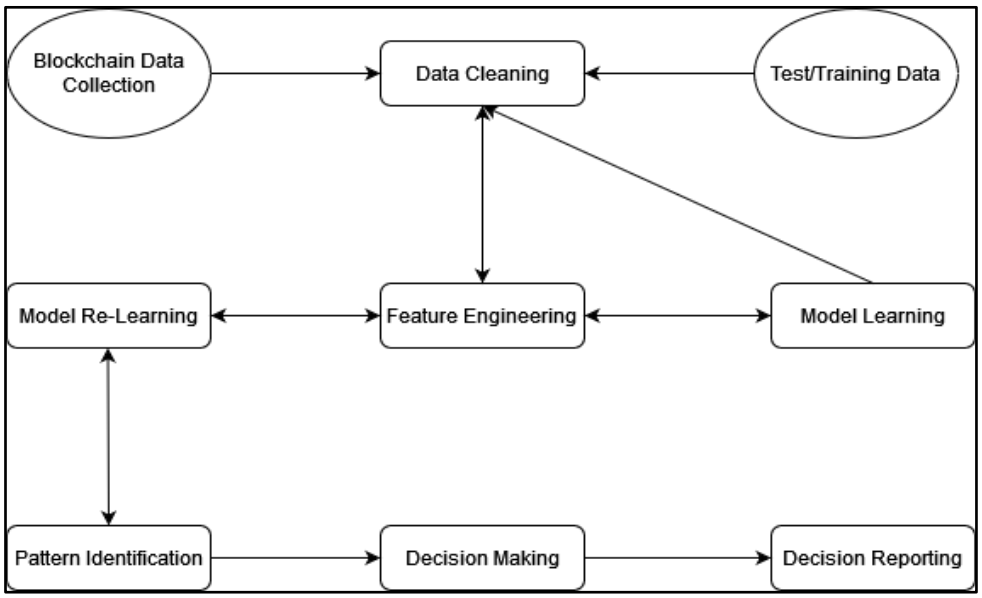

Fig. 1 The methodology's overall progression

RESULT AND DISCUSSION

The blockchain data is available on the internet. The model described is also evaluated against other comparable models, including Deep Neural Networks (DNN), Logistic Regression (LR), Gradient Boosting (GB), One-Class Support Vector Machine (OC-SVM), and Random Forest (RF). It is observed that our model surpasses these in both training efficiency and detection capabilities. However, given its reliance on a semi-supervised learning approach, the model may face constraints in recognizing new, previously undetected anomalies within the network.

CONCLUSION

In conclusion, this paper has explored the intricate landscape of anomaly detection within blockchain transactions through the lens of machine learning techniques. By harnessing the power of advanced algorithms and the analytical prowess of machine learning, we have developed a framework that not only identifies anomalies with high precision

but also provides insights into the nature and characteristics of these irregularities. The integration of blockchain heuristics has been a pivotal advancement, offering transparency and understandability in model predictions, which is often lacking in conventional models. Through rigorous comparative analysis, our methodology has demonstrated superior performance over existing models, especially in terms of detection accuracy and efficiency.

Our research underscores the significance of feature contribution analysis and the application of ensemble classifiers in enhancing the detection capabilities of machine learning models. The comparison model of DNN, LR, and GB introduced in this study has proven to be effective in balancing the dataset, thereby improving the model's sensitivity to anomalies. These innovations contribute to a more robust and reliable anomaly detection system in blockchain networks, which is critical for maintaining the integrity and security of these systems.

As blockchain technology continues to evolve and find new applications, the need for sophisticated anomaly detection mechanisms will only grow. This paper lays the groundwork for future research in this domain, encouraging the exploration of more complex models, larger datasets, and real-world applications. It is hoped that our contributions will inspire further advancements in the field, making blockchain technology safer and more reliable for users worldwide.
In summary, this study not only advances our understanding of anomaly detection in blockchain but also sets a new benchmark for the application of machine learning in this field. The methods and insights presented herein have the potential to significantly impact the development of more secure, transparent, and efficient blockchain systems, heralding a new era in digital transactions and beyond.

FUTURE WORK

Furthermore, private blockchain-based techniques for cyberattack detection may be created to guarantee that private information, including computer network logs, can be safely studied without disclosing private data.

REFERENCES

[1]. Hu, Y., Seneviratne, S., Thilakarathna, K., Fukuda, K., & Seneviratne, A. (2019). Characterizing and detecting money laundering activities on the bitcoin network. arXiv preprint arXiv:1912.12060.
[2]. Larik, A. S., & Haider, S. (2011). Clustering based anomalous transaction reporting. Procedia Computer Science, 3, 606-610.
[3]. Laws, F., & Schütze, H. (2008, August). Stopping criteria for active learning of named entity recognition. In Proceedings of the 22nd International Conference on Computational Linguistics (Coling 2008) (pp. 465-472).
[4]. Lewis, D. D., & Catlett, J. (1994). Heterogeneous uncertainty sampling for supervised learning. In Machine learning proceedings 1994 (pp. 148-156). Morgan Kaufmann.
[5]. Li, X., Cao, X., Qiu, X., Zhao, J., & Zheng, J. (2017, August). Intelligent anti-money laundering solution based upon novel community detection in massive transaction networks on spark. In 2017 fifth international conference on advanced cloud and big data (CBD) (pp. 176-181). IEEE.
[6]. Liu, X., & Zhang, P. (2010, August). A scan statistics based suspicious transactions detection model for anti-money laundering (AML) in financial institutions. In 2010 International Conference on Multimedia Communications (pp. 210-213). IEEE.
[7]. Sravan Kumar Pala, "Detecting and Preventing Fraud in Banking with Data Analytics tools like SASAML, Shell Scripting and Data Integration Studio", *IJBMV*, vol. 2, no. 2, pp. 34–40, Aug. 2019. Available: https://ijbmv.com/index.php/home/article/view/61
[8]. Liu, X., Zhang, P., & Zeng, D. (2008). Sequence matching for suspicious activity detection in anti-money laundering. In Intelligence and Security Informatics: IEEE ISI 2008 International Workshops: PAISI, PACCF, and SOCO 2008, Taipei, Taiwan, June 17, 2008. Proceedings 6 (pp. 50-61). Springer Berlin Heidelberg.
[9]. McInnes, L., Healy, J., & Melville, J. (2018). Umap: Uniform manifold approximation and projection for dimension reduction. arXiv preprint arXiv:1802.03426.
[10]. Monamo, P. M., Marivate, V., & Twala, B. (2016, December). A multifaceted approach to bitcoin fraud detection: Global and local outliers. In 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA) (pp. 188-194). IEEE.
[11]. Monamo, P. M., Marivate, V., & Twala, B. (2016, December). A multifaceted approach to bitcoin fraud detection: Global and local outliers. In 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA) (pp. 188-194). IEEE.
[12]. Association of Certified Financial Crime Specialists. (n.d.). Ousted Danske Bank CEO faces nearly $400 million lawsuit tied to historic money laundering scandal. https://www.acfcs.org/ousted-danske-bank-ceo-faces-nearly-400-million-lawsuit-tied-to-historic-money-laundering-scandal/
[13]. Feder, A., Gandal, N., Hamrick, J. T., & Moore, T. (2017). The impact of DDoS and other security shocks on Bitcoin currency exchanges: Evidence from Mt. Gox. Journal of Cybersecurity, 3(2), 137-144.

[14]. Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse attacks on {Bitcoin's}{peer-to-peer} network. In 24th USENIX security symposium (USENIX security 15) (pp. 129-144).
[15]. Nayak, K., Kumar, S., Miller, A., & Shi, E. (2016, March). Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In 2016 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 305-320). IEEE.
[16]. Van Der Merwe, J. R., Zubizarreta, X., Lukčin, I., Rügamer, A., & Felber, W. (2018, May). Classification of spoofing attack types. In 2018 European Navigation Conference (ENC) (pp. 91-99). IEEE.
[17]. Dinger, J., & Hartenstein, H. (2006, April). Defending the sybil attack in p2p networks: Taxonomy, challenges, and a proposal for self-registration. In First International Conference on Availability, Reliability and Security (ARES'06) (pp. 8-pp). IEEE.
[18]. Bharath Kumar Nagaraj, Manikandan, et. al, "Predictive Modeling of Environmental Impact on Non-Communicable Diseases and Neurological Disorders through Different Machine Learning Approaches", Biomedical Signal Processing and Control, 29, 2021.
[19]. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 1-58.
[20]. Signorini, M., Pontecorvi, M., Kanoun, W., & Di Pietro, R. (2018). Bad: blockchain anomaly detection. arXiv preprint arXiv:1807.03833.
[21]. Baqer, K., Huang, D. Y., McCoy, D., & Weaver, N. (2016). Stressing out: Bitcoin "stress testing". In Financial Cryptography and Data Security: FC 2016 International Workshops, BITCOIN, VOTING, and WAHC, Christ Church, Barbados, February 26, 2016, Revised Selected Papers 20 (pp. 3-18). Springer Berlin Heidelberg.
[22]. Yin, H. S., & Vatrapu, R. (2017, December). A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning. In 2017 IEEE international conference on big data (Big Data) (pp. 3690-3699). IEEE.
[23]. Aziz, R. M., Baluch, M. F., Patel, S., & Ganie, A. H. (2022). LGBM: a machine learning approach for Ethereum fraud detection. International Journal of Information Technology, 14(7), 3321-3331.
[24]. Elmougy, Y., & Manzi, O. (2021, December). Anomaly detection on bitcoin, ethereum networks using gpu-accelerated machine learning methods. In 2021 31st International Conference on Computer Theory and Applications (ICCTA) (pp. 166-171). IEEE.
[25]. Signorini, M., Pontecorvi, M., Kanoun, W., & Di Pietro, R. (2020). BAD: A blockchain anomaly detection solution. IEEE Access, 8, 173481-173490.
[26]. Ofori-Boateng, D., Dominguez, I. S., Akcora, C., Kantarcioglu, M., & Gel, Y. R. (2021). Topological anomaly detection in dynamic multilayer blockchain networks. In Machine Learning and Knowledge Discovery in Databases. Research Track: European Conference, ECML PKDD 2021, Bilbao, Spain, September 13–17, 2021, Proceedings, Part I 21 (pp. 788-804). Springer International Publishing.
[27]. Bhowmik, M., Chandana, T. S. S., & Rudra, B. (2021, April). Comparative study of machine learning algorithms for fraud detection in blockchain. In 2021 5th international conference on computing methodologies and communication (ICCMC) (pp. 539-541). IEEE.
[28]. Tang, H., Jiao, Y., Huang, B., Lin, C., Goyal, S., & Wang, B. (2018). Learning to classify blockchain peers according to their behavior sequences. IEEE Access, 6, 71208-71215.
[29]. Sayadi, S., Rejeb, S. B., & Choukair, Z. (2019, June). Anomaly detection model over blockchain electronic transactions. In 2019 15th international wireless communications & mobile computing conference (IWCMC) (pp. 895-900). IEEE.
[30]. Vyas, Bhuman. "Ensuring Data Quality and Consistency in AI Systems through Kafka-Based Data Governance." *Eduzone: International Peer Reviewed/Refereed Multidisciplinary Journal* 10.1 (2021): 59-62.
[31]. Naseer, S., Saleem, Y., Khalid, S., Bashir, M. K., Han, J., Iqbal, M. M., & Han, K. (2018). Enhanced network anomaly detection based on deep neural networks. IEEE access, 6, 48231-48246.
[32]. Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: an ensemble of autoencoders for online network intrusion detection. arXiv preprint arXiv:1802.09089.
[33]. Cui, L., Su, X., Ming, Z., Chen, Z., Yang, S., Zhou, Y., & Xiao, W. (2020). CREAT: Blockchain-assisted compression algorithm of federated learning for content caching in edge computing. IEEE Internet of Things Journal, 9(16), 14151-14161.
[34]. Srivastav, P. Nguyen, M. McConnell, K. A. Loparo and S. Mandal, "A Highly Digital Multiantenna Ground-Penetrating Radar (GPR) System," in IEEE Transactions on Instrumentation and Measurement, vol. 69, no. 10, pp. 7422-7436, Oct. 2020, doi: 10.1109/TIM.2020.2984415.
[35]. Jhurani, Jayesh. "Revolutionizing Enterprise Resource Planning: The Impact Of Artificial Intelligence On Efficiency And Decision-making For Corporate Strategies." International Journal of Computer Engineering and Technology (IJCET) 13, no. 2 (2022): 156-165.
[36]. Jhurani, Jayesh. "Driving Economic Efficiency and Innovation: The Impact of Workday Financials in Cloud-Based ERP Adoption." International Journal of Computer Engineering and Technology (IJCET) Volume 13, Issue 2 (May-August 2022): 135-145. Article ID: IJCET_13_02_017. Available online at

https://iaeme.com/Home/issue/IJCET?Volume=13&Issue=2. ISSN Print: 0976-6367, ISSN Online: 0976–6375. DOI: https://doi.org/10.17605/OSF.IO/TFN8R.

[37]. Kanungo, Satyanarayan. "Edge Computing: Enhancing Performance and Efficiency in IoT Applications." International Journal on Recent and Innovation Trends in Computing and Communication 10, no. 12 (December 2022): 242. Accessed Month Day, Year. http://www.ijritcc.org.

[38]. Kanungo, Satyanarayan. "Hybrid Cloud Integration: Best Practices and Use Cases." International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), vol. 9, no. 5, May 2021, pp. 62-70. Available at: http://www.ijritcc.org