

# Cryptocurrency fraud detection through classification techniques

Nrusingha Tripathy<sup>1</sup>, Sidhanta Kumar Balabantaray<sup>2</sup>, Surabi Parida<sup>2</sup>, Subrat Kumar Nayak<sup>1</sup>

<sup>1</sup>Department of Computer Science and Engineering, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, India

<sup>2</sup>Department of Computer Science and Engineering, Gandhi Institute for Education and Technology, Bhubaneswar, India

## Article Info

### Article history:

Received Nov 3, 2023

Revised Jan 19, 2024

Accepted Feb 2, 2024

### Keywords:

Anomaly detection

Classification techniques

Cryptocurrency

Financial data

Prediction

## ABSTRACT

Ethereum and its native cryptocurrency, Ether, have played a worthy attention in the development of the blockchain and cryptocurrency space. Its programmability and smart contract capabilities have made it a foundational platform for decentralized applications and innovations across various industries. Because of its anonymous and decentralized structure, the hotheaded expansion of cryptocurrencies in the payment space has created both enormous potential and concerns related to cybercrime, including money laundering, financing terrorism, illegal and dangerous services. As more financial institutions attempt to integrate cryptocurrencies into their networks, there is an increasing need to create a more transparent network that can withstand these kinds of attacks. In this work, we are using different classification techniques, such as logistic regression (LR), random forest (RF), k-nearest neighbors (KNN), adaptive boosting (AdaBoost), and extreme gradient boosting (XGBoost) for Ethereum fraud detection. The dataset we are using includes rows of legitimate transactions done using the cryptocurrency Ethereum as well as known fraudulent transactions. The "XGBoost" model, which is noteworthy, detects variations that might attract notice and prevent potential issues in this chore.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



## Corresponding Author:

Nrusingha Tripathy

Department of Computer Science and Engineering, Siksha 'O' Anusandhan (Deemed to be University)

Bhubaneswar 751030, India

Email: nrusinghatripathy654@gmail.com

## 1. INTRODUCTION

Since cryptocurrencies were first introduced ten years ago and have become widely used as a substitute for conventional payment methods, their user base has grown exponentially. Even though it is quite popular, the majority of organizations and governments are dubious about its adoption as a standard form of payment. This is due to the fact that these transactions are decentralized, anonymous, and unstable, which makes them a prime target for many cybercrimes, including money laundering, providing risqué or illegal services, supporting terrorist organizations, and Ponzi schemes. Therefore, as more institutions try to integrate bitcoin into their systems, it is essential to recognize these behaviors and create a bitcoin transaction network that is more resistant to fraud [1], [2].

Despite the fact that the data on cryptocurrencies, especially bitcoin, is accessible to everyone, the anonymization of the data makes it impossible for anybody to connect fraudulent or illegal transaction labels to the networks. Classification techniques are a type of supervised machine learning method used to categorize data into predefined classes or labels. These techniques are commonly used for tasks like image recognition, spam email detection, sentiment analysis, and fraud detection. Aziz *et al.* [3], using light gradient boosting machine (LGBM) technique to efficiently uncover fraudulent transactions, basically make

a comparison between their measurements and the LGBM method. Extreme gradient boosting (XGBoost) and LGBM techniques exhibit the highest accuracy; however, LGBM performs somewhat better, achieving 98.60% for the given dataset. By adjusting the hyper-parameters of the LGBM further, an accuracy of 99.03% is attained. Dutta *et al.* [4] aim to find evidence of fraud and deceit in Ethereum transaction procedures. Using generalized Luroth series maps, an artificial neural network called ChaosNet enables us to achieve this functionality. Because of the high levels of chaotic activity among neurons, ChaosNet leverages some of the greatest features of biological neuronal networks to achieve difficult classification tasks that are better than those of conventional neural networks (CNN). It requires a substantially smaller amount of training data. ChaosNet's capability has been effectively utilized. To further serve the objectives of this investigation, ChaosNet has been combined with a number of well-known machine learning (ML) techniques.

For the purpose of detecting Ethereum fraud, we are employing a variety of classification approaches in this work, including logistic regression (LR), random forest (RF), k-nearest neighbors (KNN), adaptive boosting (AdaBoost), and extreme gradient boosting (XGBoost). The dataset we are working with contains rows of known fraudulent transactions as well as transactions made using the cryptocurrency Ethereum. The important "XGBoost" model detects variations that might attract notice and prevent issues. The following is a summary of the paper's contribution: i) for the purpose of detecting Ethereum fraud, we are employing a variety of classification approaches in this study and ii) to identify and stop fraud with cryptocurrencies.

## 2. RESEARCH METHOD

Cryptocurrency fraud detection is a critical task in the world of digital currencies since cryptocurrency transactions are anonymous and decentralized [5], [6]. To detect and prevent cryptocurrency fraud, we used different classification techniques in this work. This dataset includes rows including both legitimate and known fraudulent Ethereum transactions. In order to identify dishonest and dubious individuals, our study looks at Ethereum's unusual transactions or characteristics. This dataset includes rows including both legitimate and known fraudulent Ethereum transactions. In fact, Ethereum (ETH) is one of the most well-known and often-used cryptocurrencies, and it has a big market share. Developers can write and run smart pacts that have circumstances of agreement directly put into code by means of Ethereum's blockchain technology. Ethereum now has a market value of over 17% of the \$1.2 trillion worldwide cryptocurrency market. Ethereum and the original cryptocurrency vary in a few key ways [7], [8]. Ethereum is meant to be something more than merely a store of wealth and a medium of trade, in contrast to Bitcoin (BTC). Rather, Ethereum is a blockchain-based, decentralized computer network. The complete work implementation process is depicted in Figure 1.

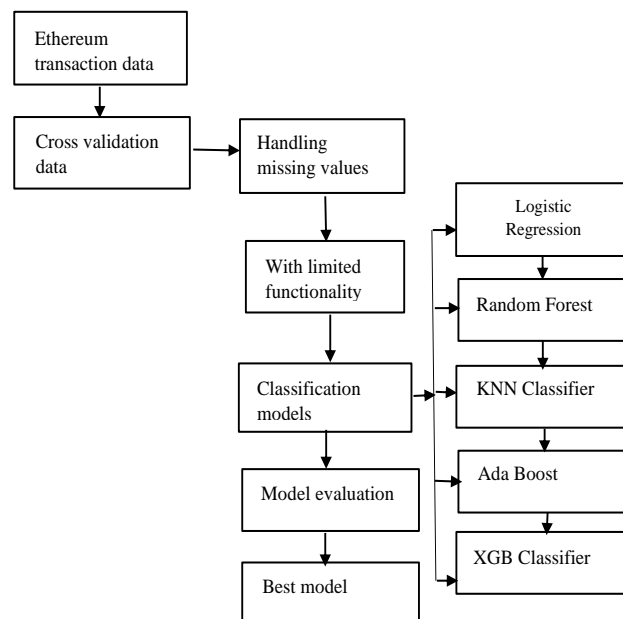


Figure 1. Work flow diagram

Due to this feature, the Ethereum platform has seen the development of numerous decentralized applications, which has increased its uptake and popularity [9], [10]. Ethereum request for comment 20 (ERC-20) governs token creation on the Ethereum blockchain, allowing them to be exchanged for other tokens from smart contracts. The standard protocol known as ERC-20 is used to create tokens based on Ethereum that may be used and distributed inside the Ethereum network. Initially we taken Ethereum transaction dataset then we go for cross validation of our dataset it aids in determining how effectively a model will function with fresh, untested data. Making the most of the data that is available in a small dataset is a situation in which cross-validation comes in handy [11], [12]. The kind of data determines which procedure should be used to handle missing values, the extent of missingness, and the goals of our analysis or modeling. It is important to carefully consider the potential impact of handling missing data in a particular way on the validity and interpretability of our results. Following the completion of pre-processing, we input the dataset into the various categorization models that we have used here. We assess the model using metrics such as recall F1-Score, accuracy, and precision. The identification of bitcoin fraud is a continuous process that requires awareness and a variety of approaches to reduce risks and preserve the reliability of cryptocurrency systems. The method of classification selected is contingent on factors like the nature of the data (e.g., structured, unstructured, text, and images), the number of classes, the availability of labeled data, and the specific requirements of the problem [13].

### 3. PROPOSED MODEL

New risks have surfaced in addition to the ease brought about by the quick advancements in information and technology. Attackers have altered their goal, method, and kind of assault due to their fast adaptation to new technology [14], [15]. A new generation of security procedures is required for governmental organizations and institutions, commercial corporations, and ordinary internet users to deal with these risks. A collection of procedures and algorithms known as classification techniques are applied to group data into specified classes or categories [16]. Each item in a batch of data is classified, using classification, into one of a predetermined set of classes or groupings. In order to predict categorical labels, a model or classifier is built for the data analysis task classification. The goal of classification is to forecast each example in the data with accuracy for the intended class. Dataset collection containing the known class assignments is the starting point for a classification task. For example, by utilizing observed data for several loan applicants over time, it could be possible to create a categorization model that forecasts credit risk [17]. Order is not indicated by discrete classifications. For forecasting models with numerical targets, regression analysis is employed instead of categorization.

The majority of scams draw inspiration from offline models, like Ponzi schemes, which are 150-year-old frauds that mimic high-yield outlay programs and allow users to cash out only if they bring in enough new members to cover the scheme's profit. Consequently, early investors profit from the insolvency of the most recent ones. The credibility of Ethereum and the entire cryptocurrency ecosystem is harmed by these scams. Cryptocurrencies are typically ranked according to their relative size in the market using their market capitalization, which is determined by multiplying their current price by their circulating supply. Changes in circulation supply and price variations can cause volatility in market cap rankings. Regression analysis determines whether variables are statistically important in describing the variation in the variable that is dependent by examining the coefficients of the variables that are independent. Regression analysis is a strong and adaptable technology with uses in many different industries. It offers a methodical approach to predict outcomes, comprehend and analyze the interactions between variables, and guide decision-making procedures.

The average mean between send transactions is shown in Figure 2; mean values are on the x-axis, while density is on the y-axis. In a similar vein, Figure 3 displays the average mean between received transactions, with mean values plotted on the x- and density-y-axes. ERC-20 tokens have played a pivotal role in various blockchain-based applications by providing a standardized and interoperable way to represent and exchange digital assets on the Ethereum network [18], [19]. Regression analysis evaluates the overall fit of the model and estimates the regression coefficients of each factor in the equation by using statistical techniques. The fraud detection histogram plot, with the number of generated contracts on the x axis and the y axis's total fraud count, is displayed in Figure 4. The number of classes, the availability of labeled data, the type of data, and the particular needs of the task all influence the classification approach that is used.

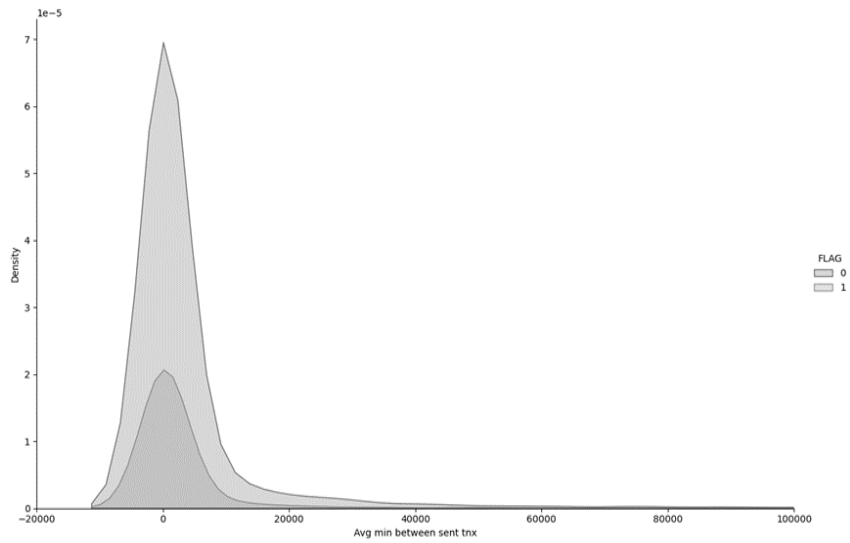


Figure 2. Average mean between send transactions

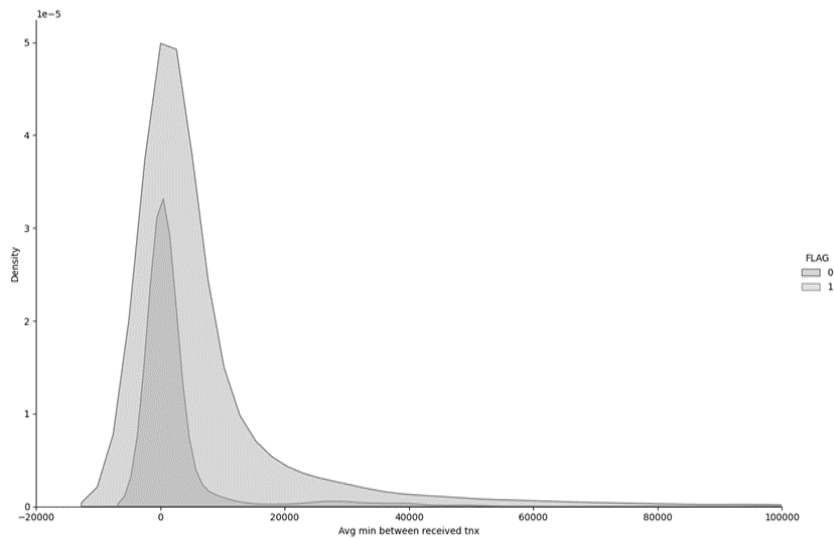


Figure 3. Average min between received transactions

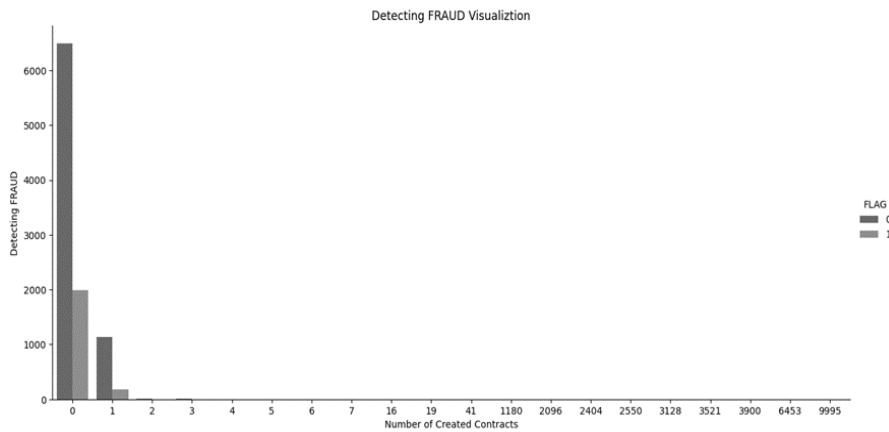


Figure 4. Detecting fraud visualization

#### 4. RESULT ANALYSIS

Even though using cryptocurrencies like Ethereum to conduct transactions is growing in popularity, fraud and other illegal activities are still frequent [20], [21]. The majority of scams draw inspiration from offline models, allowing participants to cash out only if they bring in enough new members to cover the scheme's profit. Consequently, early investors profit from the insolvency of the most modern ones [22], [23]. A statistical technique called regression analysis is utilized to look at the relationship between a number of independent variables and one or more dependent variables. The credibility of Ethereum and the whole cryptocurrency community is harmed by these frauds. For Ethereum fraud detection in this study, we use logistic regression, random forest classifiers, KNN classifiers, AdaBoost classifiers, and XGB classifiers. The XGBoost resampling algorithm for sampling outliers is given in Table 1.

Table 1. XGBoost resampling algorithm for sampling outliers

Algorithm 1
Give: $j\_pos$ and $j\_neg$ occurrences of both the positive and negative class;
R_pos vector of magnitude len ( $j\_pos$ )
R_neg vector of magnitude len ( $j\_neg$ )
While $I \in j\_pos$ do XGB[i] ← Calculate the t XGB of j;
While $k \in XGB[j]$ do F_pos[K] + ← 1;
end while
while $t \in j\_neg$ do XGB[t] ← Calculate the z XGB of t
while $j \in XGB [t]$ do F_neg[K] + ← 1
end while
$M_{Fpos} \leftarrow \text{Mean} (F\_pos);$
$DP_{Fpos} \leftarrow \text{Standard deviation of} (F\_pos);$
$M_{Fneg} \leftarrow \text{Mean} (F\_neg);$
$DP_{Fneg} \leftarrow \text{Standard deviation of} (F\_neg);$
$Cutpos \leftarrow (M_{Fpos} - DP_{Fpos});$
$Cutneg \leftarrow (M_{Fneg} - DP_{Fneg});$
while $j \in j\_pos$ do
if $F\_pos[j] < Cutpos$ then
end if
end while
while $t \in j\_neg$
end if
end while

##### 4.1. Metrics for evaluation

In the context of binary classification algorithms, such as those employed to identify fraud or Ponzi schemes, the words true positive (TP), true negative (TN), false positive (FP), and false negative (FN) are frequently used. The terms "TP" and "TN" denote the quantity of Ponzi scheme contracts that are accurately detected and the quantity of contracts that are not Ponzi schemes, FP for the quantity of smart indentures that do not include Ponzi schemes but are mistakenly identified, and FN for the quantity of contracts involving Ponzi outlines that are mistakenly estimated as non-Ponzi outline indentures [24]. These are the definitions of precision, recall, and F1-Score, which we use to determine the model's performance:

$$\text{Precision} = \frac{TP}{TP+FP} \quad (1)$$

$$\text{Recall} = \frac{TP}{TP+FN} \quad (2)$$

$$\text{F1-Score} = 2 * \frac{\text{Precision} * \text{recall}}{\text{Precision} + \text{recall}} \quad (3)$$

In comparison to the other models, the XGB classifier yields higher results in terms of accuracy. It has a 98% accuracy rate, which is higher than other results. The XGBoost model's confusion matrix is displayed in Figure 5. The F1-Score of the XGB classifier is shown in Figure 6 and Figure 7 displays the ROC curve. The performance of each classification model is listed in Table 2. Because cryptocurrency transactions are decentralized and anonymous, detecting cryptocurrency fraud is an essential challenge in the realm of digital currencies [25], [26]. In this paper, we apply several categorizations approaches to identify and stop bitcoin fraud. This dataset contains rows including known fraudulent as well as authentic Ethereum transactions. Ethereum request for comment 20 (ERC-20) is a commonly used specification for developing and using fungible tokens on the Ethereum network. Like conventional currencies or assets, these tokens are

used to signify digital assets that are exchangeable. ERC-20 tokens have become a fundamental building block of the Ethereum ecosystem, as they enable the creation and management of various digital assets, including cryptocurrencies and utility tokens [27], [28]. Prices for cryptocurrencies can fluctuate significantly over brief periods of time. Price changes can be influenced by a variety of factors, including macroeconomic trends, regulatory developments, market sentiment, and technological breakthroughs. These rules ensure compatibility and interoperability among different tokens, wallets, and decentralized applications (DApps) within the Ethereum network [29]–[32].

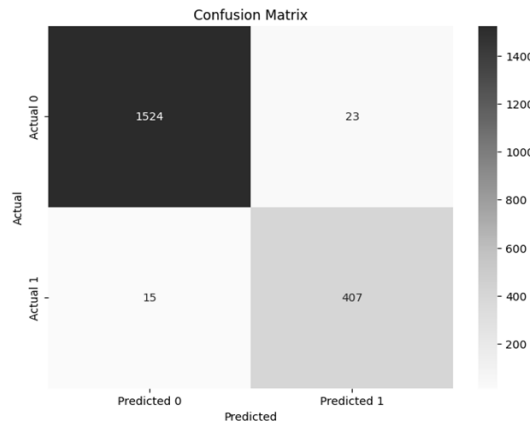


Figure 5. Confusion matrix

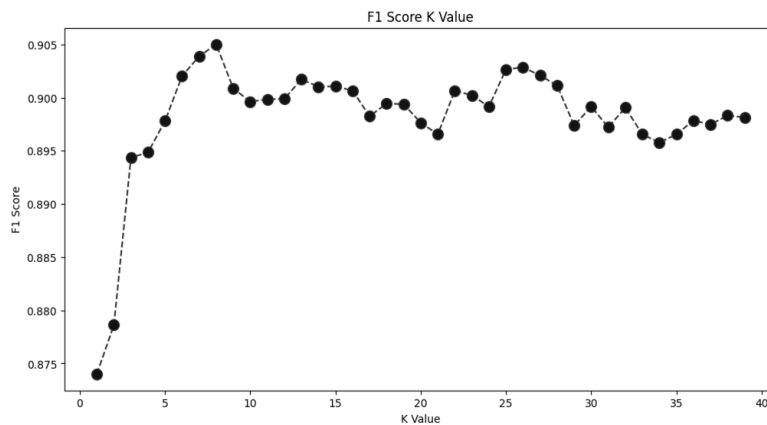


Figure 6. F1-Score plot of XGB classifier

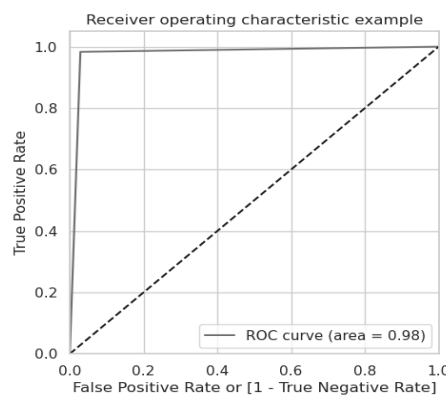


Figure 7. ROC curve of XGB classifier

Table 2. Performance analysis

Model Name	Precision	Recall	F1-Score	Accuracy
Logistic Regression	0.339	0.869	0.488	0.61
Random Forest	0.929	0.938	0.933	0.97
KNN Classifier	0.807	0.734	0.769	0.90
Ada Boost Classifier	0.899	0.893	0.896	0.96
XGB Classifier	0.946	0.964	0.955	0.98

## 5. CONCLUSION

The effectiveness of a cryptocurrency fraud detection system will be contingent on eminence of the data, the choice of structures, the selection of classification algorithm, and the model's tuning. Regularly update the model and adapt to emerging fraud patterns to enhance the system's effectiveness. A noteworthy model called "XGBoost" detects variations that might attract notice and prevent issues. In machine learning, a variety of algorithms and classification strategies are available, each with unique advantages and disadvantages. The type of data and the particular issue we are attempting to address will determine which classification strategy is best. The cryptocurrency network normalizes its users' activity by using several addresses and digital wallets. Because of their numerous addresses, these individuals resemble regular users in several ways. Finding a little deviation in these users' behavior is necessary to detect this kind of anomaly, also known as an in-disguise anomaly. Anomaly detection in earlier research was accomplished by the extraction of novel characteristics that depend on the user's digital wallets being connected. Nevertheless, the suggested approach makes use of collaborative anomaly detection. To improve the classification performance, more sophisticated feature extraction and temporal debiasing methods can be applied. Using our technique on more datasets will be helpful for research in the future.




## REFERENCES

- [1] P. Monamo, V. Marivate, and B. Twala, "Unsupervised learning for robust Bitcoin fraud detection," in *2016 Information Security for South Africa - Proceedings of the 2016 ISSA Conference*, Aug. 2016, pp. 129–134, doi: 10.1109/ISSA.2016.7802939.
- [2] L. Liu, W. T. Tsai, M. Z. A. Bhuiyan, H. Peng, and M. Liu, "Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum," *Future Generation Computer Systems*, vol. 128, pp. 158–166, Mar. 2022, doi: 10.1016/j.future.2021.08.023.
- [3] R. M. Aziz, M. F. Baluch, S. Patel, and A. H. Ganie, "LGBM: a machine learning approach for Ethereum fraud detection," *International Journal of Information Technology (Singapore)*, vol. 14, no. 7, pp. 3321–3331, Jan. 2022, doi: 10.1007/s41870-022-00864-6.
- [4] A. Dutta, L. C. Voumik, A. Ramamoorthy, S. Ray, and A. Raihan, "Predicting cryptocurrency fraud using ChaosNet: The Ethereum manifestation," *Journal of Risk and Financial Management*, vol. 16, no. 4, p. 216, Mar. 2023, doi: 10.3390/jrfm16040216.
- [5] K. G. Al-Hashedi and P. Magalingam, "Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019," *Computer Science Review*, vol. 40, Art. no. 100402, May 2021, doi: 10.1016/j.cosrev.2021.100402.
- [6] H. Baek, J. Oh, C. Y. Kim, and K. Lee, "A model for detecting cryptocurrency transactions with discernible purpose," in *International Conference on Ubiquitous and Future Networks, ICUFN*, Jul. 2019, vol. 2019-July, pp. 713–717, doi: 10.1109/ICUFN.2019.8806126.
- [7] E. Jung, M. Le Tilly, A. Gehani, and Y. Ge, "Data mining-based Ethereum fraud detection," in *Proceedings - 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019*, Jul. 2019, pp. 266–273, doi: 10.1109/Blockchain.2019.00042.
- [8] M. Bartoletti, S. Lande, A. Loddo, L. Pompianu, and S. Serusi, "Cryptocurrency scams: Analysis and perspectives," *IEEE Access*, vol. 9, pp. 148353–148373, 2021, doi: 10.1109/ACCESS.2021.3123894.
- [9] N. Tripathy, S. Hota, and D. Mishra, "Performance analysis of bitcoin forecasting using deep learning techniques," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 31, no. 3, pp. 1515–1522, Sep. 2023, doi: 10.11591/ijeecs.v31.i3.pp1515-1522.
- [10] T. Ashfaq *et al.*, "A machine learning and blockchain based efficient fraud detection mechanism," *Sensors*, vol. 22, no. 19, Art. no. 7162, Sep. 2022, doi: 10.3390/s22197162.
- [11] H. Kanezashi, T. Suzumura, X. Liu, and T. Hirofuchi, "Ethereum fraud detection with heterogeneous graph neural networks," *arxiv.org/abs/2203.12363*, Mar. 2022.
- [12] A. A. Amponsah, A. F. Adekoya, and B. A. Weyori, "A novel fraud detection and prevention method for healthcare claim processing using machine learning and blockchain technology," *Decision Analytics Journal*, vol. 4, Art. no. 100122, Sep. 2022, doi: 10.1016/j.dajour.2022.100122.
- [13] N. Tripathy, S. Parida, and S. K. Nayak, "Forecasting stock market indices using gated recurrent unit (GRU) based ensemble models: LSTM-GRU," *International Journal of Computer and Communication Technology*, pp. 85–90, Jul. 2023, doi: 10.47893/ijcct.2023.1443.
- [14] Y. Kumar, "AI techniques in blockchain technology for fraud detection and prevention," in *Security Engineering for Embedded and Cyber-Physical Systems*, CRC Press, 2022, pp. 207–224, doi: 10.1201/9781003278207-14.
- [15] A. Sallam, T. H. Rassem, H. Abdu, H. Abdulkareem, N. Saif, and S. Abdullah, "Fraudulent account detection in the Ethereum's network using various machine learning techniques," *International Journal of Software Engineering and Computer Systems*, vol. 8, no. 2, pp. 43–50, Jul. 2022, doi: 10.15282/ijsecs.8.2.2022.5.0102.
- [16] F. Poursafaei, G. B. Hamad, and Z. Zilic, "Detecting malicious Ethereum entities via application of machine learning classification," in *2020 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2020*, Sep. 2020, pp. 120–127, doi: 10.1109/BRAINS49436.2020.9223304.




- [17] V. Patel, L. Pan, and S. Rajasegarar, "Graph deep learning based anomaly detection in Ethereum blockchain network," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12570 LNCS, Springer International Publishing, 2020, pp. 132–148, doi: 10.1007/978-3-030-65745-1\_8.
- [18] B. Podgorelec, M. Turkanović, and S. Karakatič, "A machine learning-based method for automated blockchain transaction signing including personalized anomaly detection," *Sensors (Switzerland)*, vol. 20, no. 1, Art. no. 147, Dec. 2020, doi: 10.3390/s20010147.
- [19] K. Ariya, S. Chanaim, and A. Y. Dawod, "Correlation between capital markets and cryptocurrency: impact of the coronavirus," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 6, pp. 6637–6645, Dec. 2023, doi: 10.11591/ijece.v13i6.pp6637-6645.
- [20] A. Viswam and G. Darsan, "An efficient bitcoin fraud detection in social media networks," *2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, Kollam, India, 2017, pp. 1-4, doi: 10.1109/ICCPCT.2017.8074262.
- [21] N. Tripathy, S. Hota, S. Prusty, and S. K. Nayak, "Performance analysis of deep learning techniques for time series forecasting," in *2023 International Conference in Advances in Power, Signal, and Information Technology, APSIT 2023*, Jun. 2023, pp. 639–644, doi: 10.1109/APSIT58554.2023.10201734.
- [22] R. Tan, Q. Tan, P. Zhang, and Z. Li, "Graph neural network for Ethereum fraud detection," in *Proceedings - 12th IEEE International Conference on Big Knowledge, ICBK 2021*, Dec. 2021, pp. 78–85, doi: 10.1109/ICKG52313.2021.00020.
- [23] R. F. Ibrahim, A. M. Elian, and M. Ababneh, "Illicit account detection in the Ethereum blockchain using machine learning," in *2021 International Conference on Information Technology, ICIT 2021 - Proceedings*, Jul. 2021, pp. 488–493, doi: 10.1109/ICIT52682.2021.9491653.
- [24] O. I. Jacinta, A. E. Omolara, M. Alawida, O. I. Abiodun, and A. Alabdultif, "Detection of Ponzi scheme on Ethereum using machine learning algorithms," *Scientific Reports*, vol. 13, no. 1, Oct. 2023, doi: 10.1038/s41598-023-45275-0.
- [25] T. Hu *et al.*, "Transaction-based classification and detection approach for Ethereum smart contract," *Information Processing and Management*, vol. 58, no. 2, p. 102462, Mar. 2021, doi: 10.1016/j.ipm.2020.102462.
- [26] N. Nayyer, N. Javaid, M. Akbar, A. Aldegheishem, N. Alrajeh, and M. Jamil, "A new framework for fraud detection in bitcoin transactions through ensemble stacking model in smart cities," *IEEE Access*, vol. 11, pp. 90916–90938, 2023, doi: 10.1109/ACCESS.2023.3308298.
- [27] N. Tripathy, P. Satapathy, S. Hota, S. K. Nayak, and D. Mishra, "Empirical forecasting analysis of bitcoin prices: A comparison of machine learning, deep learning, and ensemble learning models," *International Journal of Electrical and Computer Engineering Systems*, vol. 15, no. 1, pp. 21–29, Jan. 2024, doi: 10.32985/ijeces.15.1.3.
- [28] H. Jang and J. Lee, "An empirical study on modeling and prediction of bitcoin prices with Bayesian neural networks based on blockchain information," *IEEE Access*, vol. 6, pp. 5427–5437, 2017, doi: 10.1109/ACCESS.2017.2779181.
- [29] K. Rathan, S. V. Sai, and T. S. Manikanta, "Crypto-currency price prediction using decision tree and regression techniques," in *Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019*, Apr. 2019, vol. 2019-April, pp. 190–194, doi: 10.1109/icoei.2019.8862585.
- [30] M. Ali and S. Shatabda, "A data selection methodology to train linear regression model to predict bitcoin price," in *2020 2nd International Conference on Advanced Information and Communication Technology, ICAICT 2020*, Nov. 2020, pp. 330–335, doi: 10.1109/ICAICT51780.2020.9333525.
- [31] S. Balabantaray, S. Parida, S. Nayak, and N. Tripathy, "A comparative analysis of cryptocurrency exchange rate prediction using deep learning techniques," *International Journal of Smart Sensor and Adhoc Network*, vol. 4, no. 1, Art. no. 3, Dec. 2023.
- [32] B. Chen, F. Wei, and C. Gu, "Bitcoin theft detection based on supervised machine learning algorithms," *Security and Communication Networks*, vol. 2021, pp. 1–10, Feb. 2021, doi: 10.1155/2021/6643763.

## BIOGRAPHIES OF AUTHORS






**Nrusingha Tripathy**    received the MCA degree in computer science from Ravenshaw University, Cuttack, Odisha, India in 2018, the M.Tech degree in computer science from the Utkal University, Bhubaneswar, Odisha, India in 2020. He is currently pursuing his Ph.D. in computer science and engineering at Institute of Technical Education and Research (I.T.E.R.) in Siksha 'O' Anusandhan Deemed to be University, Bhubaneswar, India and has published 5 Conference. Moreover, 10 journal papers have been published. Although, he has 5 years of teaching experience. He can be contacted at email: nrusinghatripathy654@gmail.com.






**Sidhanta Kumar Balabantaray**    received the B.Tech degree in computer science and engineering from MITS, Rayagada, Odisha, India in 2011, M.Tech in computer science from Berhampur University, Odisha, India in 2014. He is currently working as an assistant professor in the Department of Computer Science and Engineering at Gandhi Institute for Education and Technology (GIET), Baniatangi, India. He has more than 12 years of academic experience. His research interests include data mining, machine learning, deep learning, and internet of things. He has published six journal papers. He can be contacted at email: sidhantakumarbalabantaray@gmail.com.





**Surabi Parida**    received the B.Tech degree in computer science from Koustuv Institute of Self Domain (KISD), BBSR, Odisha, India in 2018, M.Tech in computer science from Utkal University, Bhubaneswar, Odisha, India in 2020. She is currently working as an assistant professor in the Department of Computer Science and Engineering at Gandhi Institute for Education and Technology (GIET), Baniatangi, India. She has more than 2 years of academic experience. Her research interests include data mining, machine learning, and deep learning, IoT. She has published four journal papers. She can be contacted at email: parida.surabi220@gmail.com.



**Subrat Kumar Nayak**    received the degree in MCA from Biju Patnaik University of Technology, Odisha, India in 2010, M.Tech in computer science from Utkal University, Bhubaneswar, Odisha in 2012. He is currently pursuing his Ph.D. in computer science and engineering at SOA University, Bhubaneswar, India. He has published 10 papers in various International Journals and International conferences. He qualified UGC Net in the year 2012. He has more than 6 years of academic experience and 3 years of govt experience. He can be contacted at email: subratsilicon28@gmail.com.