ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 4, April 2024

Enhancing Blockchain Trustworthiness through Machine Learning Models

[1] Volladapu Sowmya, [2] Kothuri Leela Naga Amar Sai Krishna, [3] Mahankali Satwik Janardhan, [4] Ramesh A

[1] [2] [3] [4] Department of CSE, Vardhaman College of Engineering Hyderabad, India
Corresponding Author Email: [1] volladapusowmya2002@gmail.com, [2] mahankalisatwikj@gmail.com, [3] klnamarsaikrishna@gmail.com, [4] ramesh.adavelli@vardhaman.org

Abstract*— In the realm of blockchain technology, maintaining the network's integrity and reliability depends critically on the identification of fraudulent transactions. Such fraudulent operations damage trust in blockchain-based solutions like cryptocurrencies in addition to posing hazards to the economy. This study uses a broad range of machine learning methods to tackle the problem of fraud detection in blockchain networks. The efficacy of different sets of algorithms like Multilayer Perceptron (MLP), Naive Bayes, AdaBoost, Decision Tree, Random Forest, and Support Vector Machine (SVM), as well as Logistic Regression, is methodically examined. Our models are trained and assessed against the "Crypto Investment Fund Directory" dataset using the "Ethereum Fraud Detection Dataset," which includes both legitimate and fraudulent transactions. The principal aim of this undertaking is to enhance the dependability of blockchain networks by facilitating the prompt identification and resolution of fraudulent acts, thereby fostering confidence and trust among relevant parties.

Keywords*—Blockchain Network, Fraudulent transactions, Algorithms, Machine learning, Cryptocurrencies, Crypto Investment Fund Directory, Ethereum.

I. INTRODUCTION

The potential of blockchain technology to transform several industries, including supply chain management, healthcare, and banking, has attracted a lot of attention in recent years. However, the problem of fraudulent transactions has become a major concern as blockchain-based solutions are adopted more widely [1]. The integrity of blockchain networks is compromised by fraudulent actions, which also discourage people and businesses from investing in and relying on these technologies [2].

The legitimacy of blockchain technology is still being threatened by fraudulent transactions, hence it is imperative to create reliable fraud detection systems [3]. To maintain the dependability and security of blockchain networks, build user trust, and encourage investment in blockchain-based solutions, it is imperative that fraudulent activity be identified and prevented [4].

To ensure the security and reliability of blockchain networks, foster user trust, and encourage investment, robust fraud detection systems are crucial [5]. This study investigates how well different machine learning algorithms identify and stop fraud in blockchain networks [6].

Our research effort goes beyond academic boundaries; it offers a workable answer to a big real-world issue. Blockchain technology is becoming more and more popular across industries, but the frequency of fraudulent transactions is a serious threat to the reliability and integrity of blockchain networks [7]. Our research project takes a multipronged strategy to tackle this urgent problem, fusing state-of-the-art machine learning methods with intuitive user interfaces [8].

The creation of an interface that enables users to easily train machine learning algorithms on certain datasets and then evaluate their performance forms the basis of our solution[9]. Our interface gives consumers the power to actively participate in the blockchain fraud detection process by allowing them to experiment with various algorithms and datasets [10].

We will explore the detailed methodology used in our research section below, which covers data collection and preprocessing, feature design, machine learning techniques, and network development processes. We also present the results and insights obtained through our approach, which demonstrate fraud detection accuracy and positive user experiences with our web application. Finally, we reflect on the contributions of our research, discuss the importance of fraud prediction, and encourage users to use our results to improve the security of blockchain transactions.

II. RELATED WORK

With the popularity of cryptocurrencies and digital transactions growing, fraud detection in blockchain systems is an important field of study. Traditional consensus techniques, such as proof of stake and proof of work, are excellent at validating transactions, but they have trouble identifying the parties engaged in fraudulent activity [1]. In order to tackle this problem, scholars have resorted to machine learning algorithms, which present a potentially effective remedy by utilizing past data to identify fraudulent trends within blockchain networks [2].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 4, April 2024

Several researches have examined the use of machine learning for fraud detection in blockchain systems in the literature that is currently available, with the main objective being to increase security and reliability [3]. From a blockchain viewpoint, Cai and Zhu (2016) investigated fraud detection for online firms, demonstrating how useful blockchain technology is for identifying objective frauds. They did, however, recognize that it was limited in its ability to deal with subjective frauds and suggested machine learning as a possible remedy [4].

A supervised method using machine learning techniques like Random Forests and Support Vector Machines was presented by Ostapowicz and Zbikowski (2019) for identifying fraudulent accounts on the blockchain. Their research emphasized the value of machine learning in identifying intricate patterns in blockchain data and offered insightful information on dishonest behavior [5].

Podgorelec, Turkanovic, and Karakatic (2020) devised a tailored anomaly detection method for automated blockchain transaction signature, utilizing machine learning. Their research showed that customized fraud detection techniques are feasible and underscored the significance of anomaly detection in blockchain security [6].

The study conducted by Farrugia, Ellul, and Azzopardi (2020) aimed to detect fraudulent accounts on the Ethereum blockchain. The researchers highlighted the crucial factors that contribute to fraud detection, including transaction histories and account balances. Their research emphasized the significance of transaction data nuance and the role that historical analysis plays in fraud detection [7].

By putting out a thorough strategy that makes use of a wide variety of machine learning methods, our work aims to close these gaps. Our research attempts to contribute to the creation of more practical and approachable fraud detection solutions within blockchain networks by combining various approaches and highlighting dynamic flexibility. With these initiatives, we hope to strengthen the security, dependability, and credibility of blockchain-based systems, which will eventually encourage stakeholder confidence and speed the adoption of this game-changing technology [8].

III. METHODOLOGY

A. Data Collection

This study's dataset was taken from Kaggle, a well-known supplier of different datasets. For analysis, the Ethereum Fraud Detection Dataset that is accessible on Kaggle was selected. 51 features are present in each of the 9,841 entries that make up the dataset. These properties cover a range of information on specific transactions that occur on the Ethereum blockchain network, such as transaction amounts, transaction types, and timestamps. A binary flag variable, with values of 1 signifying fraudulent transactions and 0 legitimate transactions, is another addition to the dataset that indicates the existence of fraudulent behaviour.

B. Data Pre-Processing

To make sure the Ethereum Fraud Detection Dataset was suitable for analysis, extensive pre-processing was carried out on it. This required treating non-numeric data effectively and fixing missing values. To ensure scale uniformity across variables, numerical features were standardized. To further help with dimensionality reduction, the most informative characteristics were chosen using the chi-square test. To enable efficient model training and assessment, the dataset was finally split into training, validation, and testing sets. The reliability and robustness of the studies that came after were much enhanced by these painstaking preprocessing procedures.

C. Basic Algorithm and Back-Ground

1. Logistic Regression

A popular supervised learning method that is widely used in many different industries for binary classification tasks is logistic regression. In order to ensure that predicted probabilities fall between 0 and 1, it models the likelihood of a given input belonging to one of two classes using a logistic or sigmoid function. This algorithm is used in a variety of industries, including marketing, banking, and healthcare. It helps with tasks including sickness identification, credit scoring, and churn prediction.

2. Multilayer Perceptron

Widely employed in a variety of machine learning applications, such as pattern recognition, regression, and classification, the Multilayer Perceptron (MLP) is a flexible and potent supervised learning algorithm. A multilayer network of nodes, comprising an input layer, one or more hidden layers, and an output layer, is what makes an MLP an artificial neural network (ANN) variation. Every node in one layer is connected to every other layer node, and each connection has a weight attached to it that establishes the connection strength.

3. Naive Bayes

Naive Bayes is a popular supervised learning algorithm for classification tasks, known for its simplicity and efficiency. It leverages Bayes' theorem, but with a simplifying assumption: features are considered independent of each other given the class label. This assumption, while not always accurate, often leads to surprisingly good performance, especially in scenarios with numerous features or when the independence assumption holds somewhat true. Furthermore, Naive Bayes boasts computational efficiency and requires minimal training data compared to other algorithms, making it a valuable tool for various applications.

4. Adaptive Boosting

Adaptive Boosting, or AdaBoost, is a well-known ensemble learning method for regression and classification applications. AdaBoost combines many weak learners, such

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 4, April 2024

decision trees, to create a robust model by iteratively changing the weights of misclassified instances. AdaBoost can efficiently identify intricate correlations in the data and generate precise predictions thanks to this method. AdaBoost is a popular machine learning algorithm because of its efficacy and versatility, even though it is simple. It frequently beats other algorithms in a variety of applications.

5. *Decision Tree*

Machine learning methods such as decision trees are quite flexible and can be applied to both regression and classification problems. They function by creating zones in the input space, each of which is linked to a certain class or expected value. Using a recursive procedure, each split is made according to the feature that optimizes the homogeneity of the final subgroups. Decision trees handle both category and numerical data, and they are comprehensible. But they can overfit, especially on very deep trees, therefore methods like trimming and restricting the tree's depth are frequently used to lessen the problem. Choice trees, with their straightforward design and capacity to extract intricate correlations from data, are robust models with widespread applications across multiple industries.

6. *Random Forest*

Machine learning methods such as decision trees are quite flexible and can be applied to both regression and classification problems. They function by creating zones in the input space, each of which is linked to a certain class or expected value. Using a recursive procedure, each split is made according to the feature that optimizes the homogeneity of the final subgroups. Decision trees handle both category and numerical data, and they are comprehensible. But they can overfit, especially on very deep trees, therefore methods like trimming and restricting the tree's depth are frequently used to lessen the problem. Choice trees, with their straightforward design and capacity to extract intricate correlations from data, are robust models with widespread applications across multiple industries.

7. *Support Vector Machine (SVM)*

A flexible supervised learning technique for classification and regression applications is called Support Vector Machine (SVM). SVM seeks to identify the hyperplane in the regression context that most accurately depicts the connection between the input characteristics and the target variable. It functions by locating support vectors, or data points that affect the hyperplane's position. With the introduction of kernel functions, SVM can handle both linear and non-linear interactions and is efficient in high-dimensional areas. Because of their durability and adaptability, support vector machines (SVMs) are widely used in real estate valuation for both prediction tasks and diverse dataset.

D. Evaluation Metrics

1. *Chi-Square test*

A statistical technique called the Chi-square test is employed to ascertain whether two categorical variables significantly correlate with one another. It does this by comparing the actual and predicted frequencies of each category in a contingency table, assuming that the variables are independent of one another.

This test primarily investigates whether two categorical variables, namely the two dimensions of this contingency table, are not dependent on the test statistic given by the values in this test. The test is valid if the test statistic is chi-square under the null hypothesis, especially Pearson's chi-square test and its variants.

Formula:-

$$\chi^2 = \sum \frac{(Oij - Eij)^2}{Eij}$$

Where

Oij =observed frequencies

Eij =expected frequencies i=rows

j=columns

2. *Precision*

It refers to the ability of a model to accurately identify the relevant instances from a set of all instances it predicts to be positive.More formally, precision is defined as the ratio of true positive predictions to the total number of instances predicted as positive, including both true positives and false positives.

Precision is a model performance metric that corresponds to the fraction of values that actually belong to a positive class out of all of the values which are predicted to belong to that class. Precision is also known as the positive predictive value.It is calculated using the following formula.

Formula:-

$$Precision = \frac{True\ Positives}{True\ Positives + False\ Positives}$$

Where

True Positives=instances that were correctly classified as positive by the model.

False Negatives=instances that were incorrectly classified as positive by the mode.

3. *Recall*

It is defined as the ratio of true positive predictions to the total number of actual positive instances, which includes both true positives and false negatives.

Recall is a metric that measures how often a machine learning model correctly identifies positive cases (true positives) out of all true positive samples in a data set. A return is obtained by dividing the number of true positives by the quantity of positive events.It is calculated using the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 4, April 2024

following formula.

Formula:-

$$Recall = \frac{True\ Positives}{True\ Positives + False\ Negatives}$$

Where

True Positives=instances that were correctly classified as positive by the model.

False Negatives=instances that were incorrectly classified as negative by the model, but are actually positive.

4. F-Score

It is a metric used to evaluate the performance of a classification model.It is a single scalar value that combines precision and recall into a single measure, providing a balance between the two.

The F1 score is a machine learning evaluation metric that measures the accuracy of the model.The accuracy metric counts how many times the model made a correct prediction across the entire dataset. It can only be a reliable metric if the dataset is class-balanced; that is, each class in the dataset has the same number of samples.

Formula:-

$$F = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

E. Architecture Diagram

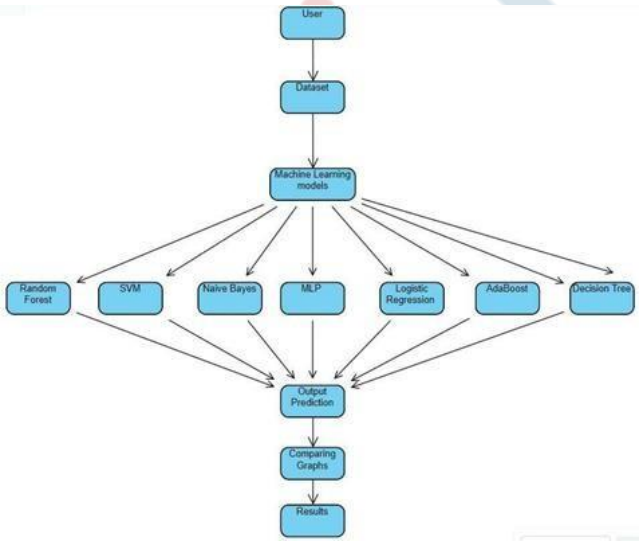

Fig-1 Architectural Flow of the Process

Fig-1 In order to initiate the project procedure, the user uploads the dataset onto the platform. When the data is uploaded, preprocessing ensures that it is ready for analysis. Preprocessing involves converting non-numeric data into numeric formats, standardizing numerical features, and filling in missing values. Following preprocessing, the dataset is divided into training and testing sets.

The information is then processed by many machine learning methods, including Random Forest, SVM, Naive Bayes, AdaBoost, Decision Tree, and MLP. Every algorithm is trained on the training set, and its performance is evaluated using metrics such as accuracy, precision, recall, and F1 score. After training and evaluation, the trained models are ready to be tested on new data.

IV. RESULTS AND DISCUSSION

The work we completed illustrated a number of outcomes. The information about the evaluation measures and the visual element is also included in this results section.

The table provides an overview of the performance metrics including accuracy, precision, recall, and F1 score for several machine learning algorithms. Each row represents a different algorithm, while each column displays a specific performance metric. The algorithms included in the analysis are MLP, Naive Bayes, AdaBoost, Decision Tree, Random Forest, SVM, and Logistic Regression.

The accuracy metric measures the overall correctness of the model's predictions. Precision represents the proportion of true positive predictions among all positive predictions made by the model. Recall, also known as sensitivity, measures the proportion of true positive predictions that were correctly identified by the model out of all actual positives. The F1 score is the harmonic mean of precision and recall, providing a balance between the two metrics.

Table-1 Evaluation Metrics of Different Models

Algorithm Name	Accuracy	Precision	Recall	F-Score
Logistic Regression	83.8	85.58318925389014	64.17183113512368	67.33212341197822
MLP	83.5	78.53395595526345	67.4779767627346	70.4181793734025
Naive Bayes	48.1	64.31265802136856	66.52512197562254	47.9646560743922
AdaBoost	92.4	89.9046089853405	84.15209727445546	88.4252291 34760068
Decision Tree	92.2	88.10914624068936	89.3561923595294	88.7097894809977
SVM	84.3	91.64893617021276	63.82488479262673	67.10464285489795
Random Forest	94.699999999	93.940800330033	90.11982743907105	91.85516328860845

For each algorithm, the corresponding cell in the table contains the value of the respective performance metric. These values are obtained from experimental results or analytical assessments conducted on the algorithms using a specific dataset or datasets.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 11, Issue 4, April 2024

The accuracy metric denotes the overall correctness of the model's predictions across all classes. Precision quantifies the proportion of true positive predictions among all positive predictions made by the model, emphasizing the model's ability to avoid false positives. Recall, also referred to as sensitivity, measures the proportion of true positive predictions correctly identified by the model out of all actual positive instances, highlighting the model's ability to capture all relevant instances. The F1 score, being the harmonic mean of precision and recall, provides a balanced assessment of the model's performance, particularly in scenarios where class imbalance exists. These metrics offer valuable insights into the effectiveness and robustness of each machine learning algorithm in accurately predicting fraudulent transactions within blockchain networks.

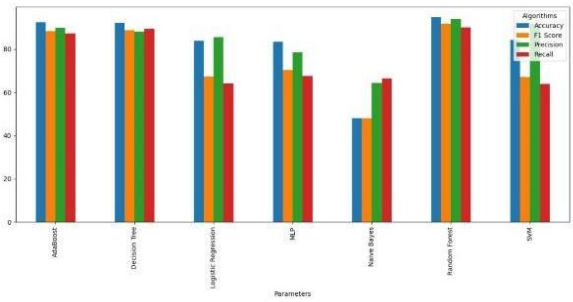

Fig-2

Fig2 the graph presents the performance comparison of different machine learning algorithms for different evaluation metrics: Accuracy**,** F1 score, precision and recall. Each algorithm is represented on the x-axis, while the y-axis shows the values of their metrics. Stakeholders can identify which algorithm excels in detecting fraudulent transactions.

In summary, the visual representation empowers stakeholders to discern which algorithm is most effective for detecting fraud, enabling them to deploy the most suitable solution for their specific needs.

V. CONCLUSION

In summary, our project addresses the important challenge of detecting fraudulent transactions on blockchain networks that have significant economic consequences and undermine trust in the cryptocurrency ecosystem. Improve the security and reliability of blockchain systems by leveraging various supervised machine learning models such as MLP, Naive Bayes, AdaBoost, Decision Trees, Random Forests, SVM, and Logistic Regression. Through extensive evaluation and testing on the Ethereum Fraud Detection Dataset and the Crypto Investment Fund Directory Dataset, our project provides valuable insight into the effectiveness of various machine learning algorithms in identifying fraudulent activity within blockchain networks.

These insights not only help improve fraud detection systems, but also provide guidance to potential investors to help them make more informed decisions about investing in blockchain-based solutions. Moreover,by developing an easy-to-use interface that allows users to experiment with different algorithms and datasets, our project promotes active participation in the fraud detection process and improves the security and reliability of blockchain technology, fosters a collaborative approach to improving overall, our research initiative represents an important step towards strengthening the integrity and trustworthiness of blockchain networks, thereby increasing stakeholder trust and encouraging the adoption of this innovation across industries.

REFERENCES

[1] Aiolli F, Conti M, Gangwal A, Polato M (2019) Mind your wallet's privacy: Identifying bitcoin wallet apps and user's actions through network trafficanalysis. DOI 10.1145/3297280.3297430

[2] Cai, Y., Zhu, D. (2016). Fraud detections for online businesses: a perspective from blockchain technology. Finance Innov, 2(20). DOI: 10.1186/s40854-016-0039-4

[3] Farrugia S, Ellul J, Azzopardi G. (2020). Detection of illicit accounts over the Ethereum blockchain. Expert Systems with Applications, 150, 113318. DOI: 10.1016/j.eswa.2020. 113318

[4] Gaihre A, Luo Y, Liu H (2018) Do bitcoin users really care about anonymity? an analysis of the bitcoin transaction graph. In: 2018 IEEE International Conference on Big Data (Big Data), IEEE, pp 1198–1207

[5] G. Franchi, A. Bursuc, E. Aldea, S. Dubuisson and I. Bloch, "Encoding the Latent Posterior of Bayesian Neural Networks for Uncertainty Quantification," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 46, no. 4, pp. 2027-2040, April 2024, doi: 10.1109/TPAMI.2023.3328829.

[6] Hu Y, Seneviratne S, Thilakarathna K, Fukuda K, Seneviratne A (2019) Characterizing and detecting money laundering activities on the bitcoin network. arXiv preprint arXiv:191212060

[7] Hyvarinen, H., Risius, M., Friis, G. (2017). A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services. Bus Inf Syst Eng, 59, 441–456.DOI: 10.1007/s12599-017 0502-4

[8] Kumar P., Gupta G.P., Tripathi R. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. *J. Syst. Archit.* 2021;**115**:101954. doi: 10.1016/j.sysarc.2020.101954

[9] Ostapowicz M., Zbikowski K. (2019). Detecting Fraudulent Accounts on Blockchain: A Supervised Approach. In: Cheng R., Mamoulis N., Sun Y., Huang X. (eds) Web Information Systems Engineering – WISE 2019. Springer, Cham. DOI: 10.1007/978-3-030 34223-4_2 .

[10] O. Günlü, M. R. Bloch, R. F. Schaefer and A. Yener, "Secure Integrated Sensing and Communication," in IEEE Journal on Selected Areas in Information Theory, vol. 4, pp. 40-53, 2023, doi: 10.1109/JSAIT.2023.3275048.

[11] Pham, Thai, Steven Lee. (2016). Anomaly detection in bitcoin network using unsupervised learning methods. arXiv:1611.03941. Retrieved from arXiv

[12] Podgorelec, B., Turkanovic, M., Karakatic, S. (2020). A Machine Learning-Based Method for Automated Blockchain

Transaction Signing Including Personalized Anomaly Detection. Sensors, 20(1), 147. DOI: 10.3390/s20010147

[13] Rahouti M, Xiong K, Ghani N (2018) Bitcoin concepts, threats, and machine-learning security solutions. IEEE Access 6:67189–6720540.

[14] Reyes-Macedo VG, Salinas-Rosales M, Garcia GG (2019) A method for blockchain transactions analysis. IEEE Latin America Transactions 17(07):1080–1087

[15] R. Bakh, V. Sarkar, J. P. Lovelin Auguskani, G. Poornima, M. N. Shetty and M. G. Raj, "Health Care and Management based on Block chain and Machine Learning," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-6, doi: 10.1109/ICECONF57129. 2023.10083757. keywords: {Telemedicine; Government; Medical treatment; Machine learning; Medical services; Knowledge discovery; Blockchains; Machine Learning; Healthcare; Blockchain; Technology}

[16] Singh, S., Singh, S. and Kajla, T. (2023), "Checking the Effectiveness of Blockchain Application in Fraud Detection with A Systematic Literature Review Approach", Grima, S., Sood, K. and Özen, E. (Ed.) Contemporary Studies of Risks in Emerging Technology, Part B (Emerald Studies in Finance, Insurance, and Risk Management), Emerald Publishing Limited, Leeds, pp. 57-86.

[17] V. Shrivastava and S. Kumar, "Utilizing Blockchain Technology in Various Application Areas of Machine Learning," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 2019, pp. 167-171, doi: 10.1109/COMITCon.2019.8862203. keywords: {Blockchain; Machine learning; Smart contracts; Supply chains; Cryptocurrency; Machine Learning; Blockchain Technology; Distributed Database}