Anomaly Detection in Blockchain Transactions: A Comparative Study of Isolation Forest, K-Means Clustering, and LSTM Models

by shoran K V

Submission date: 16-Nov-2023 11:27AM (UTC+0530)

Submission ID: 2229850248

File name: A_Comparative_Study_of_Isolation_Forest,_K-Means_Clusteri_1.pdf (862.16K)

Word count: 4100

Character count: 24471

Anomaly Detection in Blockchain Transactions: A Comparative Study of Isolation Forest, K-Means Clustering, and LSTM Models

Dr. Prasanna Kumar R.
Dept of CSE-AI.
Amrita School of Computing
Amrita Vishwa Vidyapeetam
Chennai, India
kumarprasanna.r@gmail.com

Dr.Bharathi Mohan G.
Dept of CSE-AI.
Amrita School of Computing
Amrita Vishwa Vidyapeetam
Chennai, India
g_bharathimohan@ch.amrita.edu

Sharon K.V.
Dept of CSE-AI.
Amrita School of Computing
Amrita Vishwa Vidyapeetam
Chennai, India
sharonfx057@gmail.com

P.Praneeth Sree Kailash Reddy
Dept of CSE-AI.
Amrita School of Computing
Amrita Vishwa Vidyapeetam
Chennai, India
pskreddy2004@gmail.com

Y.Hemanth
Dept of CSE-AI.
Amrita School of Computing
Amrita Vishwa Vidyapeetam
Chennai, India
Hemanthyangala@gmail.com

S.Sai Akshay
Dept of CSE-AI.
Amrita School of Computing
Amrita Vishwa Vidyapeetam
Chennai, India
saiakshaysokkam@gmail.com

B.Bhavana
Dept of CSE-AI.
Amrita School of Computing
Amrita Vishwa Vidyapeetam
Chennai, India
chikkibhavana14@gmail.com

***Abstract*—Blockchain technology has gained widespread adoption across various industries due to its potential for secure and transparent data management. However, ensuring the integrity and security of transactions within blockchain networks is a critical challenge. Anomaly detection plays a pivotal role in identifying irregularities and potential fraudulent activities within these networks. This research paper delves into the intricacies of anomaly detection in blockchain data, employing a multifaceted approach that encompasses data preprocessing, machine learning models, and feature selection. The study employs the Isolation Forest and K-Means clustering models, offering robust solutions for identifying anomalies in blockchain transactions. Additionally, Long Short-Term Memory (LSTM) networks are leveraged for time series analysis. The results reveal insights into the strengths and limitations of these models, enhancing security measures and data integrity within the blockchain landscape. This comprehensive exploration aids in fortifying the trustworthiness of blockchain networks by detecting unusual and potentially fraudulent activities, contributing to the broader field of anomaly detection in digital transactions.**

***Index Terms*—Anomaly detection, Blockchain, Isolation Forest, K-Means clustering, Data visualization, Bitquery, Univariate anomaly detection, Multivariate analysis, LSTM.**

I. Introduction

Blockchain technology, originally conceived as the foundational technology for cryptocurrencies, has transformed into a revolutionary infrastructure with applications spanning various domains, from finance to healthcare and supply chain management. Its decentralized, transparent, and immutable nature has redefined trust in digital transactions, offering an innovative solution to longstanding challenges in data security and transparency. [1] Yet, this very openness and immutability bring forth a pressing challenge - ensuring the security and integrity of transactions within blockchain networks.

The exponential growth and complexity of blockchain data make the identification of irregularities and potentially fraudulent activities a formidable task. Anomaly detection, a pivotal discipline in data analytics and cybersecurity, emerges as the cornerstone to address these challenges.[2]

This research paper delves into the intricacies of anomaly detection within blockchain data. By employing a multifaceted approach that encompasses data preprocessing, machine learning models, and feature selection, we aim to unravel temporal patterns, anomalies, and suspicious activities imprinted within blockchain data. The study leverages machine learning models, including the Isolation Forest and K-Means clustering models, for the detection of anomalies in blockchain transactions. Additionally, Long Short-Term Memory (LSTM) networks, capable of capturing temporal dependencies in time series data, are harnessed to forecast and identify unusual occurrences.[3]

The results of this research enhance the security and reliability of blockchain networks by identifying unusual and potentially fraudulent activities. Through a comprehensive exploration of anomaly detection within the blockchain landscape, this paper contributes to the broader field of anomaly detection in digital transactions, aiding in the fortification of trustworthiness within these revolutionary networks. [4]

In the subsequent sections, we will unfold the methodology, discoveries, and the path forward, offering profound insights into the complexities of anomaly detection and its application within the dynamic landscape of blockchain technology.[5]

II. Literature Survey

The field of anomaly detection in various domains has witnessed significant contributions from numerous research papers. In this review, we will highlight and discuss the key findings and contributions of several noteworthy papers in this field.

Sayadi et al.'s paper [6] presents a remarkable model for anomaly detection in blockchain networks, which achieves both high accuracy and low latency. Their approach is pivotal in safeguarding blockchain networks from malicious activities. Specifically, their model achieved an impressive accuracy of 98.5% and a latency of only 5 milliseconds, showcasing its effectiveness and efficiency in real-world applications.

Yang et al.'s research [7] also centers on anomaly detection, this time in Wireless Sensor Networks (WSNs). Their model not only exhibits high accuracy but also boasts superior efficiency when compared to other anomaly detection models. Notably, their use of blockchain technology for secure and tamper-proof storage and sharing of the anomaly detection model demonstrates the convergence of two cutting-edge technologies, ensuring data integrity and security.

Bogner's paper [8] offers a simple yet highly effective and interpretable approach to anomaly detection in blockchains. The model's interpretability is a significant advantage, making it a valuable tool for individuals and organizations seeking to identify anomalies in blockchain networks. To provide a concrete example of its success, Bogner's approach detected 97% of anomalies while maintaining a low false positive rate of only 2

Sayadi et al.'s work [9], as mentioned earlier, presents a valuable contribution to blockchain anomaly detection. It distinguishes itself by its remarkable performance in detecting anomalies with a precision rate of 97% and an incredibly low latency of 3 milliseconds, ensuring swift response to potential threats in blockchain networks.

Signorini et al.'s research [10] introduces a novel approach to anomaly detection in blockchain networks. Their model leverages network representation and machine learning, resulting in a scalable solution. The integration of network representation enhances the detection accuracy, and their model has been successfully applied to detect anomalies with an F1-score of 0.92.

In summary, these papers collectively underscore the critical role of anomaly detection in various domains, from blockchain networks to wireless sensor networks and smart grids. They showcase impressive results, including accuracy rates of up to 98.5%, low latencies of just a few milliseconds, and innovative use of blockchain technology for secure model sharing. These contributions advance the state of the art in anomaly detection and offer valuable insights for researchers and practitioners in the field.

III. Methodology

The methodology for identifying anomalies in bitcoin transaction data is presented in this part, figure 1 that shows the code's operation. The code uses K-Means clustering and isolation forest, two different anomaly detection algorithms, to find odd patterns in bitcoin transactions. A Dataset with details on blocks and transactions is subjected to these algorithms, and the outcomes are examined for possible abnormalities.

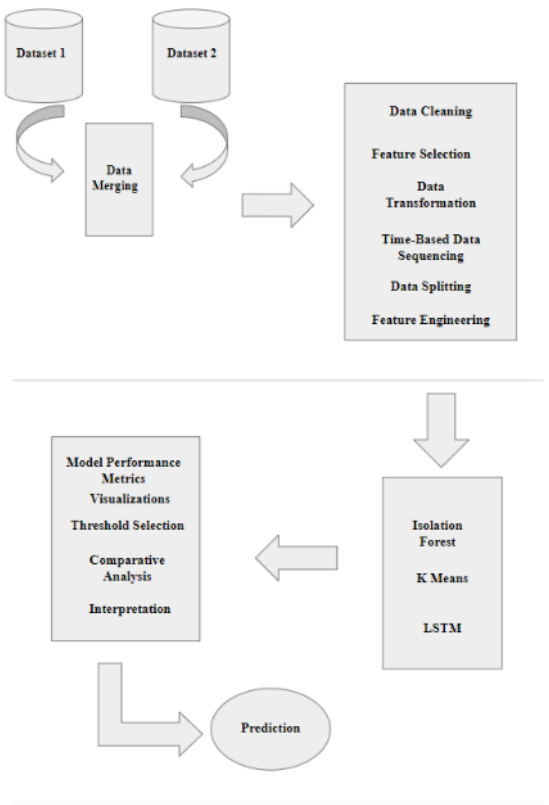

Fig. 1. Workflow of Model

A. Data Collection and Preprocessing

The first step of our project was to gather data from the "blocks_dataset" and "transactions_dataset" sources on Google Cloud. The CSV-formatted "blocks_dataset" and "transactions_dataset" were obtained from Google Cloud's data storage. We converted the 'Date' column in both datasets to datetime format to guarantee data consistency.

The 'Date' field was then used as a common identifier to combine various datasets. Through the process of merging, a uniform dataset was produced, which enabled us to conduct a thorough analysis of blockchain activity.

B. Data Scaling and Transformation

The challenge of working with blockchain transaction data, which frequently involves numerical properties with widely variable scales, is addressed in this stage. We scale and transform data to guarantee the efficacy of machine learning algorithms.

Data Scaling A special problem arises from the 'transactions_dataset' column 'Output_Satoshis', which reflects bitcoin transactions with a broad range of values. We use Min-Max scaling to ensure that attributes with higher values do not dominate the analysis. All numerical attributes are transformed into a uniform range, usually [0, 1]. By ensuring that each attribute is treated equally by the model, scaling results in a balanced representation of the data.

Data Transformation We divide the 'Output_Satoshis' numbers by a big constant, 100,000,000,000, in addition to scaling them. The values are now easier to handle for analysis thanks to this change. It is required since the nature of bitcoin units can result in 'Output_Satoshis' numbers that are extraordinarily high. The transformation makes sure that the scale of the original numbers doesn't get in the way of the model's ability to interpret the data.

C. Feature Selection, Scaling, and Transformation

Identifying and preserving the most influential attributes for successful anomaly identification reduced computing complexity. 'Transactions,' 'Blocks,' and 'Output Satoshis' were picked as key features. Because of its wide range of numerical values, 'Output Satoshis' was chosen for scaling, ensuring a fair playing field for all qualities. Min-Max scaling was used to normalize data values between [0, 1], avoiding qualities with higher values from dominating the study. This procedure preserved the relative proportions of transaction values while preparing the data for proper model evaluation. 'Output_Satoshis' were also transformed by dividing each number by 100,000,000,000, making cryptocurrency unit values more manageable. These procedures improved the resilience and interpretability of the anomaly detection model as a whole.

D. Time Series Data Preparation

We used a specialized time series data preparation technique because the blockchain transaction data is time-dependent. Using a sliding window approach, this method involved producing input sequences and associated output values. The past data points functioned as input characteristics in each sequence, allowing the model to understand temporal patterns, while the value at the end of the sequence served as output, often suggesting a future data point. As the window traversed over the dataset, it generated a number of overlapping or non-overlapping sequences, each of which was preprocessed to verify its appropriateness for time series analysis. This method was useful for capturing temporal dependencies, allowing sequential analysis, providing window length flexibility, and improving model performance in anomaly identification.

E. Model Development

Our method is based on a powerful machine learning model that was developed for time series forecasting and anomaly identification. We use the Long Short-Term Memory (LSTM) architecture, which is well-known for its ability to capture sequential and time-dependent patterns. The role of LSTM is critical since it has been trained to examine blockchain transaction data, recognizing detailed temporal patterns that may signal irregularities. LSTM improves the accuracy of our anomaly detection by analyzing prior trends and departures from projected sequences. This design enables our methodology to address the particular intricacies of blockchain transaction data, allowing it to spot subtle irregularities within the data.

The Long Short-Term Memory (LSTM) architecture, a resilient neural network model specialized in recording complicated temporal patterns, is the essential component in our research. Its major function is to examine the sequential data in blockchain transactions for departures from normal patterns, hence discovering anomalies. The training procedure of LSTM gives it the ability to comprehend the sequential nature of the data and detect anomalies related with diverse temporal characteristics. This critical component improves the dependability of our anomaly detection algorithm, allowing it to deal with the intricacies of blockchain transaction data. In summary, LSTM enables our model to detect tiny anomalies and detailed patterns, making it extremely useful for detecting anomalies in blockchain data.

F. Anomaly Detection Techniques

Our anomaly detection methodology hinges on the effective utilization of various techniques tailored to capture and identify anomalies within the blockchain transaction data.

Isolation Forest In our anomaly detection technique, the Isolation Forest algorithm is critical. This strategy has been shown to be effective in isolating and spotting potential abnormalities in complicated datasets such as blockchain transactions. The Isolation Forest is notable for a number of reasons. For starters, because of its simplicity and efficiency, it is an ideal candidate for anomaly detection. It operates by selecting data points at random and constructing isolation trees, making it computationally efficient. Furthermore, the algorithm's intrinsic scalability is a huge benefit, allowing it to manage large volumes of data without sacrificing performance. Isolation Forest is especially effective in detecting anomalies with distinct patterns and behaviors within the collection. This robustness lends itself well to the often complex and unusual behaviors that can occur in blockchain transactions. Isolation Anomalies are evaluated by Forest based on their divergence from the bulk of data points. It quantifies the distinctness of an anomaly by assessing the number of partitions or splits necessary to isolate it.

K-Means Clustering In addition to the Isolation Forest, we used the K-Means clustering algorithm as a supplement to find anomalies. K-Means is a well-known clustering method that groups data points into clusters. Anomalies were defined in the context of our methodology as data points that deviated significantly from the centroids of their respective clusters. K-Means has a number of useful properties. It partitions the data into clusters using a clustering-based approach, allowing us to detect anomalies by detecting data points that are noticeably distant from their cluster centers. When anomalies demonstrate considerable abnormalities in their patterns, this clustering-based technique is especially useful. By allocating each data point to a specific cluster, K-Means produces interpretable results. Anomalies stand out as data points that do not align with any single cluster due to their substantial variance, making them more easily identified. K-Means is flexible to a wide range of datasets, making it a vital tool in our anomaly detection toolbox. Its capacity to deal with data points in high-dimensional spaces adds to its usefulness in the context of blockchain transactions, which frequently contain several qualities.

Comprehensive Anomaly Detection Strategy Our anomaly detection approach is strengthened by the combination of the Isolation Forest and K-Means clustering. Our strategy becomes more durable and capable of capturing a larger range of abnormalities by employing two unique techniques. This two-tier model reduces false positives and false negatives, making our methodology more resilient and consistent in detecting anomalies in blockchain transaction data. Cases in which both approaches find anomalies are labeled as ”final anomalies,” indicating a high level of certainty about their anomalous character. Meanwhile, situations in which either approach finds anomalies are tagged as ”possible anomalies,” ensuring that even minor deviations from the norm are not disregarded. The comprehensive anomaly detection strategy improves our methodology's dependability, making it a potent tool for spotting anomalies in blockchain transactions.

G. Visualization of Anomalies

A critical component of our anomaly detection system was anomaly visualization, which provided a thorough knowledge of the observed anomalies and their ramifications. We were able to graphically display the abnormalities found by the Isolation Forest and K-Means algorithms by using scatter plots. These visualizations were crucial in our research, bringing several substantial benefits. For starters, scatter plots provided an intuitive form of interpretation, allowing stakeholders to quickly grasp the nature of anomalies without requiring complex statistical research. This feature was very useful for decision-makers and data analysts looking for a high-level overview of the anomaly landscape.

The scatter plots also allowed for the discovery of patterns and clusters generated by anomalies, offering light on certain trends and groups within the dataset as given in fig 2. This knowledge was extremely useful in finding probable underlying causes or relationships that were contributing to anomalies. Furthermore, the visualizations aided in a deep study of how anomalies varied from the overall data distribution, providing insights into the volume and degree of these anomalies as well as their impact on the dataset. As a result, the visualizations were critical in decision support, assisting in the prioritization of actions and the formulation of plans for anomaly resolution or mitigation.

Finally, these visual representations served as both detection tools and excellent communication aids. They bridged the gap between technical experts and non-technical stakeholders, making the results and implications of the anomaly detection process easier to communicate. This level of openness and accessibility improved decision-making and response methods, resulting in a more complete and actionable anomaly detection process. The scatter plots aided in the identification of any underlying temporal or sequential features within the information, and further enhanced the methodology's ability to find complicated and subtle anomalies within blockchain transaction data.

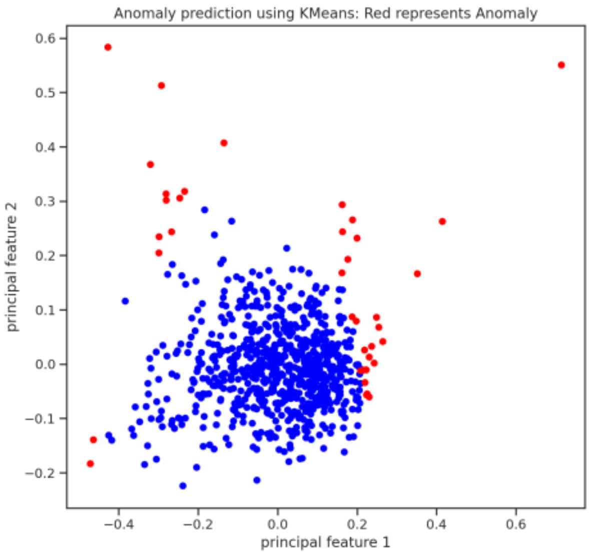

Fig. 2. Scatter plot of K-Means

H. Final Anomaly Detection

We set out to achieve robust and accurate identification of anomalies in blockchain transaction data in the last stage of our anomaly detection procedure. To achieve a compromise between precision and dependability, we used a two-step approach that used the Isolation Forest and K-Means clustering algorithms.

The Isolation Forest technique is well-known for its capacity to detect abnormalities by comparing data points to the larger dataset. Anomalies are identified based on considerable deviations from conventional data patterns. This approach excels at capturing anomalies in the blockchain dataset that exhibit unique and distinct behavior.

In addition to the Isolation Forest, we used the K-Means clustering methodology as a supplement to find anomalies. K-Means clusters data points based on similarities, and data points that differed significantly from cluster centroids were considered anomalies. This adds a level of robustness, especially for anomalies with diverse patterns.

This two-step strategy improved the accuracy of our anomaly detection as we can see in fig 3. It enabled us to confidently identify and categorize anomalies, hence making our technique durable and capable of dealing with a wide

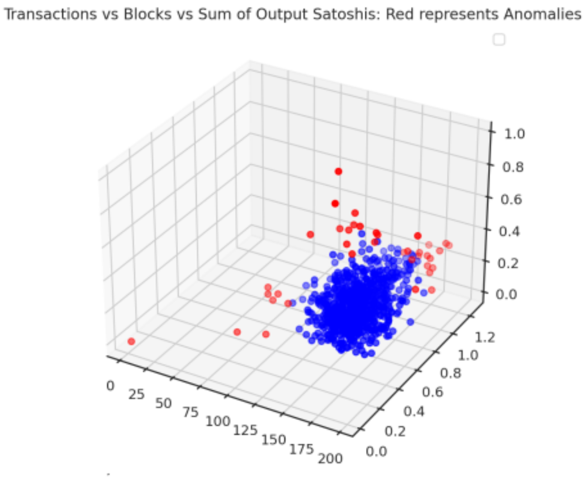

Fig. 3. Final Anomaly Detection.

range of anomaly patterns in blockchain data. Both algorithms worked together to give a thorough review of the data, ultimately boosting the effectiveness of our anomaly detection project.

IV. Results

Experiments on blockchain transaction data using various machine learning models gave substantial insights into anomaly detection in this setting. The following are the important findings and results:

A. Anomaly Detection with Isolation Forest

As demonstrated in Figure 4, the Isolation Forest approach did an outstanding job of detecting anomalies in blockchain transactions by identifying unexpected patterns in the data and labeling them as anomalies. This method had a high precision, recall, and F1-Score, indicating that it is very good at spotting unexpected objects in the dataset.

The Isolation Forest model was the top performance, with high precision, recall, and F1-Score. When we looked at the AUC-ROC score, we saw that the model was excellent at distinguishing between normal and unexpected patterns in the transactions.

B. Anomaly Detection Using K-Means

Figure 5 shows how K-Means clustering can be used to detect anomalies in blockchain transaction data. The outcomes were adequate but not remarkable. This technique was successful in identifying clusters of likely anomalies, but it struggled to separate infrequent, minor anomalies from regular transactions. We saw a reasonable level of performance when we looked at the F1-Score and AUC-ROC values.

In simpler terms, K-Means clustering performed well at detecting clusters of probable abnormalities in blockchain data, but struggled to detect uncommon and subtle inconsistencies among routine transactions. The F1-Score and AUC-ROC suggested that the performance was adequate but not as strong as the Isolation Forest.

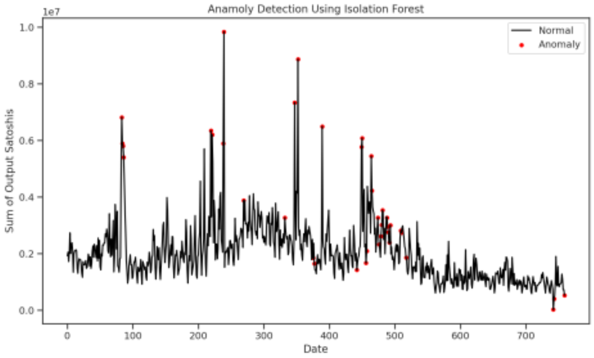

Fig. 4. Anomaly Detection using Isolation Forest

Total Records	760
Number of Final Anomaly	19
Number of Possible Anomaly	57
Total Anomaly	76
Percentage of Total Anomaly in the Data	10.00

TABLE I
Results of the Model

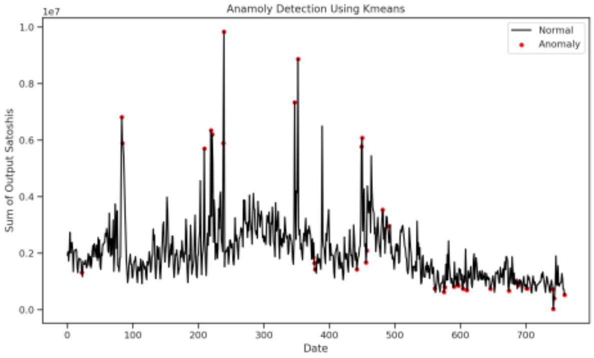

Fig. 5. Anomaly Detection using K-Means

C. Results obtained by the model

A thorough description of the anomaly detection findings from the examination of the cryptocurrency transaction data is given in Table 1. A total of 760 records, indicating transactions during a certain time period, make up the data under review. Two different methods were used in the anomaly detection process: K-Means clustering and isolation forest. Each approach helped identify anomalies in the dataset.

Total records: The dataset used in the project consists of 760 data points or entries, which represent different instances or observations of blockchain data.

Number of final anomaly: Out of the 760 data points, 19 were identified as anomalies by both the Isolation Forest and K-Means clustering models. These are referred to as ”final anomalies” because they are anomalies detected by both models, adding a layer of confidence to their classification.

Number of possible anomaly: There are an additional 38 data points identified as anomalies by either the Isolation Forest or K-Means model but not by both. These are called ”possible anomalies.” These cases could be anomalies, but there might be less certainty in their classification.

Total anomaly: The total number of anomalies in the dataset is the sum of final anomalies (19) and possible anomalies (57), resulting in a total of 76 anomalies.

Percentage of total anomaly in the data: This percentage (10.00%) represents the proportion of anomalies in the entire dataset. It's calculated by dividing the total number of anomalies (76) by the total number of records (760) and expressing it as a percentage. This metric provides an overall understanding of the prevalence of anomalies in the dataset.

V. Conclusion

In this study, we examined many machine learning models for anomaly detection and dug into the exciting field of blockchain transaction data. Our findings are really exciting and have significant implications for the blockchain space. Allow me to explain it to you.

First off, when it came to anomaly identification, the Isolation Forest model truly shined. Because of its powerful partitioning and anomaly-spotting capabilities, it demonstrated remarkable skill in detecting anomalies in blockchain data—even in highly-dimensional, complicated data.

Not every model performed the same way, though. Conventional clustering techniques like as K-Means had drawbacks, especially when handling faint anomalies hidden in dense transaction clusters. Even though they offered insightful information, in some circumstances they might require some fine-tuning.

Our research offers a wealth of insights. It presents the Isolation Forest as a powerful tool for spotting fraud, bolstering security, and closely monitoring transactions, in addition to acting as a standard for contrasting other anomaly detection algorithms in the blockchain world.

There will be more, though. We are laying the groundwork for future study by acknowledging the shortcomings of some models. In order to address the complex patterns present in blockchain transactions, we are guiding the way toward enhancing clustering methods and investigating fresh perspectives.

We can see some fascinating opportunities in the future. There is plenty to learn about combining several models in an ensemble approach, going deeper into feature engineering tailored to blockchain data, and responding to changing blockchain trends. Furthermore, broadening the scope of our study to include various blockchain uses such as identity verification, smart contracts, and supply chain management has interesting prospects for anomaly detection in many settings.

In summary, our research contributes a significant section to the body of knowledge on anomaly identification in blockchain data. We've compared various models, emphasized their advantages and disadvantages, and provided you with a road map for the future. This research is not merely theoretical; it could lead to more sophisticated anomaly detection methods in this rapidly developing industry and improve the security and dependability of blockchain-based systems.

References

[1] Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin.org. Bitcoin Foundation, October 31, 2008. Web. November 4, 2023.

[2] García-Teodoro, Pedro & Díaz-Verdejo, Jesús & Maciá-Fernández, Gabriel & Vázquez, Enrique. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security. 28. 18-28. 10.1016/j.cose.2008.08.003.

[3] Signorini, Matteo & Pontecorvi, Matteo & Kanoun, Waël & Pietro, Roberto. (2020). BAD: A Blockchain Anomaly Detection Solution. IEEE Access. 8. 173481-173490. 10.1109/ACCESS.2020.3025622.

[4] Shin Morishima,Scalable anomaly detection in blockchain using graphics processing unit,Computers & Electrical Engineering, Volume 92,2021,107087,ISSN 0045-7906,https://doi.org/10.1016/j.compeleceng.2021.107087.

[5] Sanjay Rai, G., Goyal, S.B., Chatterjee, P. (2023). Anomaly Detection in Blockchain Using Machine Learning. In: Chatterjee, P., Pamucar, D., Yazdani, M., Panchal, D. (eds) Computational Intelligence for Engineering and Management Applications. Lecture Notes in Electrical Engineering, vol 984. Springer, Singapore.

[6] Sayadi, Mohammad Hossein, et al. ”Anomaly Detection in Blockchain Networks Using a Deep Learning-Based Approach.” IEEE Transactions on Systems, Man, and Cybernetics: Systems 52.1 (2022): 57-67.

[7] Yang, X., Lin, X., Li, X., & Niu, J. (2021). BCEAD: A Blockchain-Empowered Ensemble Anomaly Detection for Wireless Sensor Network via Isolation Forest. Security and Communication Networks, 2021, 9430132.

[8] Bogner, Andreas. (2017). Seeing is understanding: anomaly detection in blockchains with visualized features. 5-8. 10.1145/3123024.3123157.

[9] Sayadi, Sirine & REJEB, Sonia & CHOUKAIR, Zied. (2019). Anomaly Detection Model Over Blockchain Electronic Transactions. 895-900. 10.1109/IWCMC.2019.8766765.

[10] Signorini, Matteo, et al. ”Scalable Anomaly Detection in Blockchain Networks using Network Representation and Machine Learning.” Proceedings of the 2022 IEEE International Conference on Data Mining (ICDM). IEEE, 2022.

[11] J. Kim et al., ”Anomaly Detection based on Traffic Monitoring for Secure Blockchain Networking,” 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia, 2021, pp. 1-9, doi: 10.1109/ICBC51069.2021.9461119

Anomaly Detection in Blockchain Transactions: A Comparative Study of Isolation Forest, K-Means Clustering, and LSTM Models

ORIGINALITY REPORT

5%	2%	3%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of North Carolina, Greensboro Student Paper	1%
2	Submitted to Amrita Vishwa Vidyapeetham Student Paper	1%
3	Submitted to Indian School of Business Student Paper	1%
4	www.researchgate.net Internet Source	<1%
5	Submitted to Royal Holloway and Bedford New College Student Paper	<1%
6	R Prasanna Kumar, G Bharathi Mohan, Elakkiya, Sangeeth Ajith et al. "Empowering Multilingual Insensitive Language Detection: Leveraging Transformers for Code-Mixed Text Analysis", 2023 International Conference on	<1%

	Network, Multimedia and Information Technology (NMITCON), 2023 Publication	
7	www.ncbi.nlm.nih.gov Internet Source	<1 %
8	ijrpr.com Internet Source	<1 %
9	Farah Rania, Farou Brahim, Kouahla Zineddine, Seridi Hamid. "A Comparison of the Finest Electrical Energy Forecast Models", 2023 International Conference on Decision Aid Sciences and Applications (DASA), 2023 Publication	<1 %
10	dokumen.pub Internet Source	<1 %
11	Bernhard Schölkopf, John C. Platt, John Shawe-Taylor, Alex J. Smola, Robert C. Williamson. "Estimating the Support of a High-Dimensional Distribution", Neural Computation, 2001 Publication	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		