IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 1, February 2024

A Literature Survey on Transaction and Phishing URL Fraud Detection in Bitcoin

Chandana C[1], Anshika V[2], Dr Kavita Patil[3]
Students, Department of Information Science and Engineering[1,2]
Professor, Department of Information Science and Engineering[3]
Global Academy of Technology, Bengaluru, India

Abstract: *The literature survey provides a comprehensive overview of the complexities surrounding cryptocurrencies, focusing on fraud detection and regulation within the global financial system. It traces the historical evolution of monetary systems, the emergence of cryptocurrencies, and regulatory approaches. Significant findings include the application of machine learning algorithms like LGBM and random forest in Ethereum fraud detection, and the effectiveness of unsupervised learning for anomaly mining in Bitcoin transactions. Novel frameworks for fraud detection through ensemble stacking models are also highlighted. The survey underscores the need for effective approaches to combat fraudulent activities within blockchain platforms, such as Ponzi schemes and phishing scams. Proposed solutions utilize methodologies like graph neural networks and ensemble learning, exhibiting high accuracy. Regulatory measures, classification technique refinement, and future research directions are emphasized to enhance fraud detection models. Overall, the survey illuminates the potential impact of cryptocurrencies on the global financial system, the challenges of unregulated circulation, and promising advancements in fraud detection and regulatory efforts within the digital economy.*

Keywords: Cryptocurrencies, Fraud Detection, Regulatory Strategies, Blockchain Technology, Machine Learning Algorithms, Ponzi Schemes, Ethereum, Financial Security, Digital Economy,Phishing scam

I. INTRODUCTION

The survey delves into machine learning's application in identifying fraud in cryptocurrency transactions, particularly within Ethereum and Bitcoin. It examines the use of machine learning, deep learning, and blockchain to counter activities like Ponzi schemes and phishing. The survey emphasizes the significance of advanced technologies, supervised and unsupervised learning, and addresses challenges such as data imbalance and privacy concerns. It also suggests future research directions, emphasizing refined feature selection, unsupervised algorithms, and tailored technologies for cryptocurrency transactions.

The study [1] addresses the rising concern of fraudulent activities on the Ethereum platform. It focuses on leveraging graph neural networks to extract features from users and transactions, classifying them as fraudulent or non-fraudulent. The study highlights challenges faced by investors due to a lack of understanding of smart contracts and prevalent fraudulent activities like phishing and smart Ponzi schemes. The study also emphasizes the superiority of graph neural networks over traditional models and suggests future research directions, including combining graph neural networks with explainable artificial intelligence and exploring custom architectures for improved accuracy and computational efficiency. The analysis [2] explores the challenge of identifying unethical and fraudulent behavior within the cryptocurrency ecosystem, particularly in the Ethereum blockchain. It delves into the analysis of fraudulent behavior using different classification techniques and machine learning algorithms, focusing on the use of k-means clustering, Support Vector Machine, and random forest classifier to construct a transaction network based on Ethereum transactional data. The study reveals that the random forest classification model achieved the best performance in identifying fraudulent behavior. The advantages of the methods used in the document include high accuracy, flexibility, and the ability to extract valuable features for analysis. The study [3] addresses the pressing need for an effective approach to identify phishing scams on the Ethereum blockchain. The authors present a three-step framework involving obtaining labeled phishing accounts and their transaction records, constructing an Ethereum transaction network,

DOI: 10.48175/IJARSCT-15395

utilizing node2vec network embedding for feature extraction, and applying a one-class support vector machine (SVM) for phishing classification. The study underscores the unique challenges of phishing on blockchain platforms, advocates for leveraging publicly accessible Ethereum transaction records, and emphasizes the superiority of network embedding methods in automatically extracting latent features.

The analysis [4] extensively explores the application of Light Gradient Boosting Machine (LGBM) for the detection of fraudulent activities within the Ethereum network. The study addresses potential threats such as Ponzi schemes, money laundering, and phishing, and proposes LGBM as an effective solution, showcasing its superior accuracy in comparison to other models like Random Forest and Multi-Layer Perceptron (MLP). The analysis also sheds light on the challenges of Ethereum fraud detection, suggesting future research directions such as refining feature selection methods and enhancing model accuracy and scalability. The study [5] delves into the application of unsupervised learning algorithms for anomaly detection in Bitcoin transactions. It evaluates various unsupervised learning algorithms, including Multivariate Gaussian distribution, One-Class SVM, Two-phase Clustering, and Isolation Forest, in the context of detecting anomalous behavior within cryptocurrency transactions. The study compares the performance of these algorithms through graphical representations and accuracy evaluations, ultimately highlighting the superiority of the Multivariate Gaussian algorithm. The analysis also includes a literature survey on related research works, showcasing diverse approaches that leverage unsupervised learning models for Bitcoin fraud detection and anomaly detection in blockchain electronic transactions. The advantages of unsupervised learning algorithms, such as their ability to handle large and complex datasets without labeled data, are outlined, along with considerations for their potential drawbacks, such as challenges in imbalanced datasets and interpretability issues. The study [6] offers a comprehensive analysis of cryptocurrencies within the context of the digital economy. It aims to assess the potential consequences of the further proliferation of cryptocurrencies in the global financial system and to identify strategies to address them. The authors delve into the historical evolution of monetary systems, from the gold standard to modern conditions, and examine the emergence and development of cryptocurrencies. They also discuss the potential use of cryptocurrencies in fraudulent schemes and evaluate the possibilities and challenges associated with the regulation of cryptographic money circulation. The document emphasizes the need to develop a legal and economic framework to regulate cryptocurrencies in the digital economy's development and highlights the opportunities and threats posed by virtual money from both economic and financial perspectives. The study also offers a critical examination of the regulatory landscape for cryptocurrencies, drawing attention to the varying approaches adopted by different countries, such as Japan, Germany, and the United States, in recognizing and regulating virtual currencies.

The analysis [7] addresses the pressing issue of identifying Ponzi schemes on the Ethereum blockchain to curb fraudulent activities causing substantial losses to investors. The study emphasizes the urgency in strengthening regulatory measures and monitoring within the blockchain market. The proposed CTRF model introduces a Code and Transaction Random Forest, leveraging features from smart contract code and transaction data to enhance the recall value for Ponzi contract identification. The document underscores the advantages of the model, including improved recall, effective data preprocessing techniques, and insightful feature analysis. However, it acknowledges challenges such as an imbalanced dataset and potential overfitting. Future research directions are suggested, including regulatory enhancements, exploration of deep learning algorithms, and addressing dataset limitations for improved generalization. The analysis [8] introduces a novel framework for detecting fraud in Bitcoin transactions, focusing on the efficiency of anomaly detection. The framework employs a stacking model with machine learning classifiers, combining Decision Tree, Naive Bayes, K-Nearest Neighbors, and Random Forest. Through ensemble learning and hyperparameter tuning using random search, the proposed model achieves impressive performance metrics, including a 97% accuracy, 98% recall, and 97% F1-score, outperforming individual classifiers. The study systematically evaluates dataset aspects, balancing techniques, hyperparameter tuning, and model construction, emphasizing the effectiveness of the ensemble Bitcoin detector (EBD) model. The analysis [9] delves into the application of machine learning algorithms, specifically the Light Gradient Boosting Machine (LGBM), for the detection of fraudulent activities within the Ethereum network. Emphasizing the surging demand for cryptocurrencies like Ethereum, the study addresses potential threats such as Ponzi schemes, money laundering, and phishing. The LGBM approach is proposed as an effective solution, showcasing its superior accuracy in comparison to other models like Random Forest and Multi-Layer Perceptron (MLP). Notably, after hyper-parameter tuning, LGBM achieves an optimized accuracy of 99.03%, attributed to its swift computation,

DOI: 10.48175/IJARSCT-15395

minimal memory consumption, and robust performance on large datasets. The document also sheds light on the challenges of Ethereum fraud detection, suggesting future research directions such as refining feature selection methods and enhancing model accuracy and scalability

II. LITERATURE SURVEY

2.1Cryptocurrencies in the Global Financial System: Problems and Ways to Overcome them (2020)

The research paper presents a comprehensive analysis of cryptocurrencies within the context of the digital economy. The study aims to assess the potential consequences of the further proliferation of cryptocurrencies in the global financial system and to identify strategies to address them. The authors delve into the historical evolution of monetary systems, from the gold standard to modern conditions, and examine the emergence and development of cryptocurrencies. They also discuss the potential use of cryptocurrencies in fraudulent schemes and evaluate the possibilities and challenges associated with the regulation of cryptographic money circulation. The document emphasizes the need to develop a legal and economic framework to regulate cryptocurrencies in the digital economy's development and highlights the opportunities and threats posed by virtual money from both economic and financial perspectives. Furthermore, the authors provide an insightful overview of the various types of fraud associated with cryptocurrencies, such as fake wallets, investment schemes, and phishing, underscoring the risks and challenges in the cryptocurrency market. The study also offers a critical examination of the regulatory landscape for cryptocurrencies, drawing attention to the varying approaches adopted by different countries, such as Japan, Germany, and the United States, in recognizing and regulating virtual currencies. Overall, the study provides a comprehensive analysis of the complexities surrounding cryptocurrencies, shedding light on their potential impact on the global financial system and the challenges posed by their unregulated circulation.

2.2 Fraudulent Behaviour Identification in Ethereum Blockchain

The research paper explores the challenge of identifying unethical and fraudulent behaviour within the cryptocurrency ecosystem, particularly in the Ethereum blockchain. The study aims to address the absence of regulation and transparency in transactions, which may lead to an increased number of fraudulent cases. The research delves into the analysis of fraudulent behaviour using different classification techniques and machine learning algorithms. It focuses on the use of k-means clustering, Support Vector Machine, and random forest classifier to construct a transaction network based on Ethereum transactional data. The results revealed that the random forest classification model achieved the best performance in identifying fraudulent behavior. The advantages of the methods used in the document include high accuracy, flexibility, and the ability to extract valuable features for analysis. However, the disadvantages include limitations in clustering algorithms, potential issues with false positives, and challenges related to data imbalance and network heterogeneity. The paper emphasizes the importance of data pre-processing and feature extraction in training and comparing the proposed models. The paper also outlines future plans to improve model reliability, such as increasing the number of fraudulent and non-fraudulent wallets for analysis and exploring the use of XG-Boost method. Additionally, the study intends to conduct a statistical significance test to ascertain differences between results and further enhance the proposed model's accuracy. Overall, the study provides a comprehensive overview of the research conducted to identify fraudulent behavior in the Ethereum blockchain, highlighting the significance of machine learning techniques and outlining future research directions.

2.3 Detecting Phishing Scams on Ethereum Based on Transaction Records [3]

The research paper addresses the pressing need for an effective approach to identify phishing scams on the Ethereum blockchain. The authors present a three-step framework involving obtaining labeled phishing accounts and their transaction records, constructing an Ethereum transaction network, utilizing node2vec network embedding for feature extraction, and applying a one-class support vector machine (SVM) for phishing classification. Experimental results reveal the model's effectiveness with an F-score of 0.846. The paper underscores the unique challenges of phishing on blockchain platforms, advocates for leveraging publicly accessible Ethereum transaction records, and emphasizes the superiority of network embedding methods in automatically extracting latent features. It discusses issues like data imbalance and network heterogeneity, introducing the one-class SVM as a solution. Furthermore, the paper delves into

ISSN 2581-9429 IJARSCT

the significance of time and amount features, explores varying embedding dimensions, and suggests future research directions. In summary, the paper contributes a comprehensive framework for detecting Ethereum phishing scams, showcasing promising results and paving the way for advancements in blockchain security and fraud detection research.

2.4 LGBM: a machine learning approach for Ethereum fraud detection [4]

The research paper delves into the application of machine learning algorithms, specifically the Light Gradient Boosting Machine (LGBM), for the detection of fraudulent activities within the Ethereum network. Emphasizing the surging demand for cryptocurrencies like Ethereum, the study addresses potential threats such as Ponzi schemes, money laundering, and phishing. The LGBM approach is proposed as an effective solution, showcasing its superior accuracy in comparison to other models like Random Forest and Multi-Layer Perceptron (MLP). Notably, after hyper-parameter tuning, LGBM achieves an optimized accuracy of 99.03%, attributed to its swift computation, minimal memory consumption, and robust performance on large datasets. The paper also sheds light on the challenges of Ethereum fraud detection, suggesting future research directions such as refining feature selection methods and enhancing model accuracy and scalability. Additionally, the document provides a comprehensive overview of the dataset, data preprocessing, and experimental setup, offering a holistic understanding of the proposed LGBM model's potential in efficiently predicting Ethereum transaction frauds.

2.5 Analysis Of Unsupervised Learning Algorithms For Anomaly Mining With Bitcoin [5]

The research paper extensively explores the application of unsupervised learning algorithms for anomaly detection in Bitcoin transactions, emphasizing the growing significance of Bitcoin technology in electronic transactions and the imperative need for robust anomaly detection methods. The proposed work evaluates various unsupervised learning algorithms, including Multivariate Gaussian distribution, One-Class SVM, Two-phase Clustering, and Isolation Forest, in the context of detecting anomalous behavior within cryptocurrency transactions. The study compares the performance of these algorithms through graphical representations and accuracy evaluations, ultimately highlighting the superiority of the Multivariate Gaussian algorithm. The paper also includes a literature survey on related research works, showcasing diverse approaches that leverage unsupervised learning models for Bitcoin fraud detection and anomaly detection in blockchain electronic transactions. The advantages of unsupervised learning algorithms, such as their ability to handle large and complex datasets without labeled data, are outlined, along with considerations for their potential drawbacks, such as challenges in imbalanced datasets and interpretability issues. Future research directions are proposed, urging further exploration of hybrid approaches and the development of advanced algorithms tailored to the unique characteristics of cryptocurrency transactions. Overall, the paper serves as a comprehensive guide to the application, evaluation, and potential advancements in unsupervised learning algorithms for enhancing anomaly detection in Bitcoin transactions.

2.6 Graph Neural Networks for Ethereum Fraud Detection[6]

Charity Mwanza's thesis, "Graph Neural Networks for Ethereum Fraud Detection," submitted to the University of Alabama in Huntsville in May 2023, addresses the rising concern of fraudulent activities on the Ethereum platform. The research focuses on leveraging graph neural networks to extract features from users and transactions, classifying them as fraudulent or non-fraudulent. It highlights challenges faced by investors due to a lack of understanding of smart contracts and prevalent fraudulent activities like phishing and smart Ponzi schemes. The introduction provides background on Ethereum's decentralized infrastructure, smart contracts, and the prevalence of fraud in the cryptocurrency market. The methodology section details the use of graph neural networks, explaining concepts like message passing and aggregation, and outlines the dataset and preprocessing steps. The paper concludes by emphasizing the superiority of graph neural networks over traditional models and suggests future research directions, including combining graph neural networks with explainable artificial intelligence and exploring custom architectures for improved accuracy and computational efficiency. Additionally, the advantages of Ethereum and smart contracts, such as instant execution and transparency, and their disadvantages, including the challenge of tracking anonymous users, are discussed. Future research purposes include combining graph neural networks with explainable AI and exploring custom architectures to enhance accuracy and computational efficiency.

2.7 CTRF: Ethereum-Based Ponzi Contract Identification [7]

The research paper titled "CTRF: Ethereum-Based Ponzi Contract Identification" addresses the pressing issue of identifying Ponzi schemes on the Ethereum blockchain to curb fraudulent activities causing substantial losses to investors. The study emphasizes the urgency in strengthening regulatory measures and monitoring within the blockchain market. The proposed CTRF model introduces a Code and Transaction Random Forest, leveraging features from smart contract code and transaction data to enhance the recall value for Ponzi contract identification. The document underscores the advantages of the model, including improved recall, effective data preprocessing techniques, and insightful feature analysis. However, it acknowledges challenges such as an imbalanced dataset and potential overfitting. Future research directions are suggested, including regulatory enhancements, exploration of deep learning algorithms, and addressing dataset limitations for improved generalization. In summary, the CTRF model contributes significantly to Ponzi contract detection on Ethereum, offering valuable insights for fraud prevention and regulatory improvements in the blockchain ecosystem.

2.8 Comparative Study of Machine Learning Algorithms for Fraud Detection in Blockchain [8]

The research paper presents a comprehensive comparative study on the integration of supervised machine learning algorithms for fraud detection in blockchain technology. It begins by highlighting the economic impact and vulnerability of blockchain networks to fraudulent transactions, advocating for the necessity of effective detection methods. The proposed system addresses blockchain's limitations in subjective fraud detection by leveraging supervised learning techniques. The literature survey emphasizes the use of supervised machine learning in identifying fraudulent activities in blockchain, setting the stage for the methodology section, which details the comparison of various models, including Logistic Regression, Multilayer Perceptron, Naive Bayes, Adaboost, Decision Tree, SVM, Random Forest Classifier, and Neural Network. The implementation phase covers pre-processing, model building, training, and performance evaluation. The document concludes by affirming the effectiveness of supervised learning for fraud detection and suggests future research avenues, such as exploring unsupervised algorithms and scrutinizing fraudulent activities in private blockchains. Notably, the study offers insights into the advantages of enhanced fraud detection and a comparative analysis while acknowledging challenges like vulnerability to subjective fraud and computational complexities. Future purposes include a comparative study of unsupervised algorithms, examination of private blockchain fraud, and ongoing advancements in fraud detection technology, collectively contributing valuable insights to the intersection of machine learning and blockchain fraud detection. Overall, the document serves as a valuable resource for researchers and practitioners in the evolving field of blockchain technology and fraud mitigation.

2.9 Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum [9]

The research paper addresses the prevalent issue of Ponzi schemes on the Ethereum blockchain. The authors propose a method for detection by collecting real-world samples and extracting features from smart contracts. They employ a Random Forest model, utilizing machine learning techniques, and conduct extensive experiments, demonstrating its superiority in detecting smart Ponzi schemes over traditional methods. The model exhibits high precision, emphasizing its accuracy in distinguishing fraudulent contracts. The study highlights the challenges posed by the lack of regulation in the blockchain space and the exploitation of information asymmetry among investors. Future purposes include the development of an early warning system and providing reusable research data sets for ongoing studies. In conclusion, the research offers a comprehensive approach to identify and monitor smart Ponzi schemes, emphasizing the need for regulatory measures and investor education to combat fraudulent activities in blockchain technology.

2.10 Tracing Cryptocurrency Scams: Clustering Replicated Advance-Fee and Phishing Websites [10]

The research paper investigates the pervasive issue of cryptocurrency scams, particularly advance-fee and phishing schemes targeting unsuspecting individuals in the cryptocurrency market. Utilizing the DBSCAN clustering technique, the study reveals that the same entities orchestrate multiple instances of similar scams, creating a deceptive façade of genuine blockchain activity. The analysis of fund flows indicates victims often send funds from fiat-accepting exchanges, while scam entities cash out through various channels like exchanges, gambling sites, and mixers. The

DOI: 10.48175/IJARSCT-15395

research also highlights the evolution of scams, showcasing new advance-fee tactics that exploit legitimate presentations to deceive victims.Advantages of the research include the identification of distinct scam types, uncovering organized campaigns, and utilizing blockchain analysis to trace fund movements. However, limitations include a focus on specific scam types and a lack of explicit prevention strategies. Future purposes could involve developing automated identification techniques, exploring prevention strategies, and fostering industry collaboration to enhance security measures. In conclusion, the paper provides crucial insights into cryptocurrency scams, emphasizing the need for comprehensive understanding and preventive strategies to protect users and improve industry integrity.

2.11 Phishing Detection in Blockchain Transaction Networks Using Ensemble Learning [11]

The research paper introduces a deep learning-based approach to identify phishing attacks in blockchain transaction networks. Leveraging methods like Long Short-Term Memory (LSTM), Bi-directional LSTM (Bi-LSTM), and convolutional neural network LSTM (CNN-LSTM), the authors evaluate their models on a dataset comprising malicious and benign addresses from the Ethereum blockchain. In addition to the research paper, the document discusses the broader landscape of blockchain technology, emphasizing its potential applications in finance, e-Governance, IoT, and smart home technologies. It addresses security and privacy concerns associated with blockchain, proposing the use of deep learning methods to enhance system security. The study compares the proposed ensemble learning approach with existing methodologies, highlighting its advantages in accuracy, adaptability to evolving attack patterns, and effectiveness in handling various phishing techniques. Furthermore, it compares favorably to previous studies, showcasing superior accuracy, recall, precision, and f-score results. The paper also provides insights into the advantages and disadvantages of blockchain technology. It highlights security, transparency, efficiency, and decentralization as notable strengths, while acknowledging challenges related to scalability, interoperability, regulatory uncertainty, and energy consumption. Future purposes of blockchain technology are discussed, including its potential impact on decentralized finance (DeFi), IoT security, supply chain management, smart contracts, and identity management. In summary, the study contributes a groundbreaking approach to phishing detection in blockchain transaction networks through ensemble learning. The broader discussion acknowledges the multifaceted nature of blockchain technology, emphasizing its strengths, challenges, and promising future applications. The research aligns with the ongoing efforts to enhance security and efficiency in blockchain systems, providing valuable insights for both academia and industry.

2.12 A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism[12]

The research paper titled "A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism" by Tehreem Ashfaq et al., published in Sensors in 2022, addresses the escalating issues of fraud and anomalies in the Bitcoin network. The paper introduces a robust fraud detection model that combines machine learning algorithms, including XGboost and random forest, with blockchain technology to enhance security in financial transactions. The proposed model incorporates data balancing techniques, machine learning algorithms, and a blockchain-based smart contract for transaction prediction and classification. Security features such as decentralization, integrity, non-repudiation, availability, and trust are discussed, and the model's resilience against double-spending and Sybil attacks is demonstrated. The system is proven effective in detecting fraudulent transactions, contributing significantly to financial security. However, challenges include the computational requirements of privacy-preserving encryption techniques and potential centralization issues with cloud-based data storage. Future research directions include refining the model to address privacy challenges and security threats, improving machine learning model robustness, and exploring advanced technologies for enhanced fraud detection and security in financial transactions and IoT-driven smart cities. Overall, the paper offers a promising solution to security and fraud detection challenges in blockchain-based transactions, paving the way for further advancements and applications.

2.13 Dissecting Ponzi schemes on Ethereum: identification, analysis, and impact [13]

The research paper provides a comprehensive examination of Ponzi schemes operating on the Ethereum platform. It delves into their historical context, migration to digital platforms like Ethereum, and adaptation to smart contract technology. Various types of Ponzi schemes, such as array-based pyramid schemes, tree-based pyramid schemes, handover schemes, and waterfall schemes, are categorized and analyzed in terms of their functionalities, vulnerabilities, and deceptive advertising tactics.The authors present a systematic methodology for identifying and analyzing these schemes, involving the collection of contracts, analysis of source code, and detection of hidden Ponzi schemes based on bytecode similarity. Security vulnerabilities within the smart contracts, deceptive advertising strategies, and the discrepancies between promised returns and actual payouts are highlighted throughout the document.Statistical data on the impact of Ponzi schemes on Ethereum, including the total amount of invested ether, number of transactions, and user involvement, is provided. Case studies like DianaEthereum-x1.8, Dynamic Pyramid, and Treasure Chest illustrate the fraudulent nature of these schemes and the significant disparities between promised returns and actual payouts.Advantages of the document include its comprehensive analysis, systematic methodology, and statistical insights into Ponzi schemes on Ethereum. However, it may be challenging for general readers due to technical language and complex statistical analysis.Future purposes of the document could involve using its insights to develop intervention policies, improve smart contract security, and inform regulatory efforts surrounding Ponzi schemes on blockchain platforms.

2.14 Cryptocurrency Scams: Analysis and Perspectives[14]

The research paper offers a comprehensive analysis of cryptocurrency scams, aiming to effectively categorize and detect them while proposing guidelines for enhanced user protection. It addresses the exponential growth of cryptocurrencies and the challenges posed by cybercriminals exploiting their pseudonymity features. The study highlights the scarcity of reliable public data sources and the absence of a standard taxonomy for scams, hindering precise scam classification. To counter these challenges, the researchers collected and homogenized data from various public sources to build a uniform dataset of cryptocurrency scams. They developed a novel taxonomy and implemented a tool to automatically recognize and classify scams. The study covers various types of cryptocurrency scams, including Ponzi schemes, malware, fake services, advance-fee scams, and money laundering, collected from sources like BadBitcoin and BitcoinAbuse. Advantages of the study include the introduction of a novel taxonomy, dataset creation, tool development for automatic classification, and proposed policy guidelines for user protection. However, challenges such as unreliable data sources, the absence of a standard taxonomy, and inaccurate scam reports are acknowledged.Future purposes suggested by the study include the development of enhanced detection tools, refining the taxonomy of cryptocurrency scams, and further implementation of policy guidelines for user protection. Overall, the research provides valuable insights into understanding and combating cryptocurrency scams while indicating areas for future research and development to address existing challenges and improve user protection in the cryptocurrency ecosystem.

2.15 A New Framework for Fraud Detection in Bitcoin Transactions Through Ensemble Stacking Model in Smart Cities [15]

The research paper introduces a novel framework for detecting fraud in Bitcoin transactions, focusing on the efficiency of anomaly detection. The framework employs a stacking model with machine learning classifiers, combining Decision Tree, Naive Bayes, K-Nearest Neighbors, and Random Forest. Through ensemble learning and hyperparameter tuning using random search, the proposed model achieves impressive performance metrics, including a 97% accuracy, 98% recall, and 97% F1-score, outperforming individual classifiers. The study systematically evaluates dataset aspects, balancing techniques, hyperparameter tuning, and model construction, emphasizing the effectiveness of the ensemble Bitcoin detector (EBD) model. It compares optimization techniques and balancing methods, highlighting the superiority of random search and ADASYN-TL, respectively. While demonstrating high accuracy in detecting fraudulent transactions, the framework is noted for its time complexity and computation cost. Future directions may involve further optimizing the model, extending its application to other domains, and integrating advanced technologies like blockchain and artificial intelligence.

DOI: 10.48175/IJARSCT-15395

III. ANALYSIS TABLE

NAME OF THE PAPER	YEAR OF PUBLICATIO N	ALGORITHMS	FINDINGS
Cryptocurrencies in the Global Financial System: Problems and Ways to Overcome them	2020	Supervised machine learning algorithms for fraud detection in blockchain technology.	Cryptocurrency impact on global financial system ,Potential use of cryptocurrencies in fraudulent schemes cryptocurrencies
Fraudulent Behaviour Identification in Ethereum Blockchain	2020	k-means clustering Support Vector Machine Random Forest Classifier	Systematic methodology for identifying Ponzi schemes, Security vulnerabilities within smart contracts
Detecting Phishing Scams on Ethereum Based on Transaction Records	2020	Light Gradient Boosting Machine (LGBM)	Three-step framework for detecting Ethereum phishing scams, Challenges of phishing on blockchain platforms
LGBM: a machine learning approach for Ethereum fraud detection	2022	Multivariate Gaussian distribution,One-Class SVM Two-phase Clustering, Isolation Forest	Security, transparency, efficiency, and decentralization as strengths ,Challenges related to scalability, interoperability, and energy consumption
Analysis Of Unsupervised Learning Algorithms For Anomaly Mining With Bitcoin	2021	Decision Tree,Naive Bayes K-Nearest Neighbors, Random Forest	Evaluation of unsupervised learning algorithms for anomaly detection, Comparison of algorithm performance
Graph Neural Networks for Ethereum Fraud Detection	2023	Node2vec networkembedding,One-class support vector machine (SVM)	Leveraging graph neural networks for fraud detection, Challenges faced by investors in the Ethereum platform
CTRF: Ethereum-Based Ponzi Contract Identification	2022	Random Forest Task-based content delivery	Urgency in strengthening regulatory measures and monitoring within the blockchain market, Introduction of Code and Transaction Random Forest model
Comparative Study of Machine Learning Algorithms for Fraud Detection in Blockchain	2022	DBSCAN clustering technique	Comparison of various machine learning models,Future research directions
Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum	2021	XGboost,Random Forest	They employ a Random Forest model, utilizing machine learning techniques, The model exhibits high precision

DOI: 10.48175/IJARSCT-15395

Tracing Cryptocurrency Scams: Clustering Replicated Advance-Fee and Phishing Websites	2020	Long Short-Term Memory (LSTM),Bi-directional LSTM (Bi-LSTM), Convolutional Neural Network LSTM (CNN-LSTM)	Identification of distinct scam types,Utilization of blockchain analysis to trace fund movements
Phishing Detection in Blockchain Transaction Networks Using Ensemble Learning	2023	DBSCAN clustering technique	Comparison of proposed ensemble learning approach with existing methodologies, Advantages of the ensemble learning approach
A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism	2022	DBSCAN clustering technique	Introduction of a robust fraud detection model,Incorporation of machine learning algorithms and blockchain technology
Dissecting Ponzi schemes on Ethereum: identification, analysis, and impact	2017	-	Categorization and analysis of various types of Ponzi schemes,Historical context and adaptation to smart contract technology
Cryptocurrency Scams: Analysis and Perspectives	2021	Ensemble learning with Decision Tree, Naive Bayes, K-Nearest Neighbors, and Random Forest	Comprehensive analysis of cryptocurrency scams, Proposed policy guidelines for user protection
A New Framework for Fraud Detection in Bitcoin Transactions Through Ensemble Stacking Model in Smart Cities	2023	Random Forest Classifier	Introduction of a novel framework for detecting fraud in Bitcoin transactions, Evaluation of ensemble stacking model performance

IV. CONCLUSION

The papers provides a comprehensive and in-depth analysis of fraudulent activities within the cryptocurrency ecosystem, with a particular focus on the Ethereum blockchain. It encompasses various research papers that explore the identification, analysis, and impact of Ponzi schemes, phishing scams, and other fraudulent behaviors. The studies employ a range of methodologies, including machine learning algorithms, graph neural networks, and ensemble learning, to detect and classify fraudulent transactions and smart contracts. Additionally, the papers address the challenges and opportunities associated with blockchain technology, the potential consequences of the proliferation of cryptocurrencies in the global financial system, and the need for regulatory measures to combat fraudulent activities. Overall, the papers offers valuable insights into the complexities of cryptocurrency scams, the potential impact on the financial system, and the ongoing efforts to enhance security and fraud detection in blockchain technology. The document serves as a valuable resource for researchers, practitioners, and policymakers in the evolving field of cryptocurrency fraud mitigation..

REFERENCES

[1]. G. Luchkin, O. L. Lukasheva, N. E. Novikova, V. A. Melnikov,,A. V. Zyatkova, and E. V. Yarotskaya, ‘‘Cryptocurrencies in the global financial system: Problems and ways to overcome them,’’ in Proc. Russian Conf. Digit. Economy Knowl. Manag. (RuDEcK), 2020.

[2]. K. Lašas, G. Kasputytė, R. Užupytė, and T. Krilavičius, ‘‘Fraudulent behaviour identification in Ethereum blockchain,’’ in Proc. CEUR Workshop, Inf. Soc. Univ. Stud., Kaunas, Lithuania, 23, Apr. 2020.

[3]. Q. Yuan, B. Huang, J. Zhang, J. Wu, H. Zhang, and X. Zhang, ‘‘Detecting phishing scams on Ethereum based on transaction records,’’ in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), Oct. 2020.

[4]. R. M. Aziz, M. F. Baluch, S. Patel, and A. H. Ganie, ‘‘LGBM: A machine learning approach for Ethereum fraud detection,’’ Int. J. Inf. Technol.,vol. 14, no. 7, pp. 3321–3331, Dec. 2022, doi: 10.1007/s41870-022-00864-6

[5]. G. D. Arya, K. V. S. Harika, D. V. Rahul, S. Narasimhan, and A. Ashok, ‘‘Analysis of unsupervised learning algorithms for anomaly mining with Bitcoin,’’ in Machine Intelligence and Smart Systems. Berlin, Germany: Springer, 2021.

[6]. Mwanza, Charity, "Graph neural networks for ethereum fraud detection" (2023). Theses. 449, https://louis.uah.edu/uah-theses/449

[7]. Xuezhi He , Tan Yang , and Liping Chen "CTRF: Ethereum-Based Ponzi Contract Identification", Hindawi,Security and Communication Networks,Volume 2022, Article ID 1554752, https://doi.org/10.1155/2022/1554752

[8]. M. Bhowmik, T. S. S. Chandana, and B. Rudra, ‘‘Comparative study of machine learning algorithms for fraud detection in blockchain,’’ in Proc. 5th Int. Conf. Comput. Methodologies Commun. (ICCMC), Apr. 2021.

[9]. W. Chen, Z. Zheng, E. C.-H. Ngai, P. Zheng, and Y. Zhou, ‘‘Exploiting blockchain data to detect smart Ponzi schemes on Ethereum,’’ IEEE Access, vol. 7, pp. 37575–37586, 2019.

[10]. Ross Phillips and Heidi Wilder, "Tracing Cryptocurrency Scams: Clustering Replicated Advance-Fee and Phishing Websites",2020,IEEE

[11]. Ogundokun, R.O., Arowolo, M.O., Damaševičius, R. and Misra, S., 2023, May. Phishing Detection in Blockchain Transaction Networks Using Ensemble Learning. In Telecom. Ashfaq, T, Khalid, R.Yahaya, A.S.; Aslam, S.; Azar, A.T.;

[12]. Alsafari, S, Hameed, I.A. "A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism.", Sensors 2022, 22, 7162. https://doi.org/10.3390/s22197162

[13]. Bartoletti, Massimo & Carta, Salvatore &Cimoli, Tiziana & Saia, Roberto. (2017). Dissecting Ponzi schemes on Ethereum: identification, analysis, and impact.

[14]. Bartoletti, Massimo & Lande, Stefano &Loddo, Andrea &Pompianu, Livio &Serusi, Sergio. (2021). Cryptocurrency Scams: Analysis and Perspectives. IEEE Access. 9. 1-1. 10.1109/ACCESS.2021.3123894.

[15]. Nayyer, Noor & Javaid, Nadeem & Akbar, Mariam &Aldegheishem, Abdulaziz &Alrajeh, Nabil & Jamil, Mohsin. (2023). A New Framework for Fraud Detection in Bitcoin Transactions Through Ensemble Stacking Model in Smart Cities. 10.1109/ACCESS.2023.3308298.