SCHOOL OF INFRASTRUCTURE, PROCESS ENGINEERING AND TECHNOLOGY
AND SCHOOL OF ELECTRICAL ENGINEERING AND TECHNOLOGY
FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA

Book of Proceedings IEC 2023

4th INTERNATIONAL ENGINEERING CONFERENCE

Theme

Smart Engineering and Technology Innovation for Enhancing Economic Growth

21st - 23rd MARCH 2023

Venue: NITDA ICT-HUB Federal University of Technology, Minna, Niger State - Nigeria

Edited By: Technical Sub-Committee

4th International Engineering Conference (IEC 2022)
Federal University of Technology, Minna, Nigeria

Cryptocurrency Fraud Detection: A systematic Literature review

*Hussaini, Y[1], Waziri, V.O[2], Isah, A. O[3], & Ojeniyi, J A[4]
[1]Cyber Security Science Department, Federal University of Technology, PMB 65 Minna Niger State, Nigeria
*Corresponding author email:hussaini.pg208686@st.futminna.edu.ng +2347063585009

ABSTRACT
Cryptocurrency Fraud is growing at alarming rate and spreading rapidly despite on-going mitigating efforts. This brings a necessity to find more effective solutions to detect these Frauds and prevent users from losing digital assets. This study uses the PRISMA statement as a reference so to be transparent. This paper uses a SLR to identify where recent studies in cryptocurrency fraud detection have been focused on and offers a broad perspective relating to types of Techniques, Algorithms, dataset sources used and also the categories of Fraud types in the research area within the range of 2018 to 2022. A total of 38 selected papers met the inclusion criteria based on title of articles, exclusion criteria, reading abstract and content of the selected 38 papers. Different data are extracted from these articles and recorded in an excel sheet for further analysis. Most of the paper discussed about the use of Machine Learning and Deep Learning analysis approach to analyse cryptocurrency fraud. We also identified research gaps that are further needed to be explored by the research community
Keywords: *Cryptocurrency, Fraud, Detection, Machine Learning, Deep learning*

1 INTRODUCTION

Since the prevalence of digital currencies has drawn a variety of illegal behavior, cryptocurrency theft is a rising worry. Ponzi schemes, spam scams, and the selling of stolen or fake cryptocurrencies are just a few examples of the various ways that cryptocurrency theft can manifest itself (Bao, F., & Li, X. (2019). Therefore, there is a need for efficient techniques to identify and stop bitcoin scams.

Numerous strategies for detecting bitcoin scams have been created and suggested in recent years. Utilizing machine learning algorithms, which can be taught on extensive databases of previously fraudulent transactions, is one hopeful strategy for finding trends and abnormalities that might be indicative of fraudulent activity (Kaur, M., & Singh, G. (2019).Among other ways to spot bitcoin scams is network analysis, which involves analyzing the links and patterns of transactions within a cryptocurrency network in order to identify groups of activity that may be linked with fake activity, and behavioral analysis, which employs user behavior data to identify suspect activity (Wang, Z., Chen, M., & Lee, W. C. (2018)

In this introduction, we will address the various kinds of deception that can occur in the bitcoin market, as well as the challenges and methods for identifying and stopping such deceptive actions. We will also look at the present state of the art in bitcoin scam identification and describe some of the potential future paths in this area.

1.1 TYPES OF FRAUD IN CRYPTOCURRENCY

The potential for unlawful activities, such as money trafficking and funding terrorists, to go unnoticed is one of the main worries with bitcoin scams. Since bitcoin transfers are private, it is challenging to determine who is responsible for the money and where the money came from. For instance, the imaginary money Bitcoin has been used on the dark web to enable drug trade and other illicit operations (Zohar, 2015). Another type of scam that has affected the bitcoin market is ponzi schemes. In a Ponzi scam, gains are given to early owners using funds raised from new investors rather than from profits. The plan persists as long as there are enough fresh participants to cover the profits. But eventually, as the number of new investors decreases, the plan falls apart; causing substantial loses for the later investors (SEC. (2020).

Exchanges for virtual currencies that make it easier to purchase and trade them are also prone to scams. Hackers may target these platforms to take users' money, as was the case with the high-profile Mt. Gox breach in 2014, which resulted in the theft of 850,000 Bitcoins valued over $450 million at the time (] Kharif, O. (2014).

1.2 CHALLENGES AND TECHNIQUES FOR FRAUD DETECTION IN CRYPTOCURRENCY

The bitcoin market is autonomous and worldwide, which makes it extremely difficult to spot and stop fake activity. Due to the absence of a centralized authority and governmental supervision, conventional scam detection techniques, such as those employed in the banking and finance sectors, may not be successful in the bitcoin market.

Using machine learning techniques to evaluate transaction trends and spot abnormalities that might point to dishonest behavior is one method for spotting fraud in cryptocurrency. A machine learning model, for instance, could be taught to spot suspect trends like a rapid rise in transaction traffic or the movement of money to well-known money launderers.

Utilizing network analysis to find groups of fraudulent transactions is another method for spotting bitcoin scams and suspicious activity. It is possible to spot trends that may suggest fake behavior by studying the connections between different addresses and the flow of funds .

1.3 CURRENT STATE OF THE ART IN FRAUD DETECTION IN CRYPTOCURRENCY

In recent years, there have been a number of significant advancements in the area of digital currencies scam identification. Using graph convolutional neural networks (GCNNs) to find fraudulent patterns in the blockchain, the decentralized ledger that keeps track of all bitcoin transactions, is a hopeful method. The complicated connections between various blockchain organizations can be successfully captured by GCNNs, and they can also spot suspect trends that could point to fraud (Wen, Z., Zeng, D., Li, Y., Li, H., & Lu, J. (2019). A survey on blockchain analytics. 52(1), 1-38, ACM Computing Surveys (CSUR), n.d.

The use of natural language processing (NLP) to identify phony ICOs is another potential area. (initial coin offerings). A business provides a new altcoin in return for investments through an initial coin offering (ICO). However, a lot of ICOs ended up being frauds, with the creators taking the collected funds and running (Kshetri, N. (2018). The Regulatory Challenges Affecting Initial Coin Offerings. n.d.; Journal of Financial Regulation and Compliance, 26(4), 318-333).

1.4 RELATED WORKS:

A systematic review of fraud detection methods in cryptocurrency market" by A. Alshammari and B. Mishra (2019).

In this paper, the authors review various fraud detection methods that have been proposed for the cryptocurrency market, including rule-based systems, machine learning techniques, and hybrid approaches.

"Cryptocurrency fraud detection using machine learning techniques: A systematic review" by M. Alomari and R. Al-Ayyoub (2020).

In this paper, the authors review the use of machine learning techniques for fraud detection in the cryptocurrency market. They discuss various machine learning approaches, including supervised learning, unsupervised learning, and semi-supervised learning, and provide a comparative analysis of their strengths and limitations.

"Fraud detection in cryptocurrency transactions using data mining techniques: A systematic review" by M. Raza, N. Anwar, and A. Alazab (2021).

In this paper, the authors review the use of data mining techniques for fraud detection in cryptocurrency transactions. They discuss various data mining approaches, including association rule mining, decision tree induction, and clustering, and provide a comparative analysis of their performance in detecting fraudulent activity.

1.5 RESEARCH QUESTIONS:

The following research questions were developed:

RQ1 – Which is the most frequent used Techniques in cryptocurrency Fraud detection?

RQ2 – which Algorithms have been used in the research area and what are the successful detection rates achieved?

RQ3 – What sources of dataset have been used the most in the research area?

RQ4 – What are the types of fraud existing in the cryptocurrency domain?

This systematic Literature review analysis will be used to answer the research questions above Using the PRISMA Framework which from my related works no work has been done using this framework. The PRISMA frame work is highly known for its transparency in conducting a review.

2 METHODOLOGY

To create an orderly yet responsible SLR, we use the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analysis) Statement. (Moher 2009.Pdf, n.d.). This statement encompasses two parts: an inventory and a flow schematic. The factors are useful in directing a researcher to the material that must be included on an SLR. Furthermore, movement maps help scholars ensure the transparency of the literature referenced by SLRs. This movement chart is divided into four phases;

(1) Identification,
(2) Screening,
(3) Eligibility, and
(4) Included.

To maintain openness, every stage in the PRISMA flow model is described in Fig. 1.

2.1 IDENTIFICATION STAGE

We create a search method to find appropriate publications during the identifying step. This search approach was customized to random databases using the Publish and perish Software with Google scholar search engine: and the following search terms were used:“Cryptocurrency Fraud Detection” NOT Review (included to restrict the search to a particular area). All searches were conducted from the Google Scholar database using the publish and perish tool, and by default, the rejection and inclusion criteria A1, A2, and B1 were applied to the journal database shown in Table II. The procedure was completed on November 31, 2022, and the findings of the inquiry are shown in Table II.

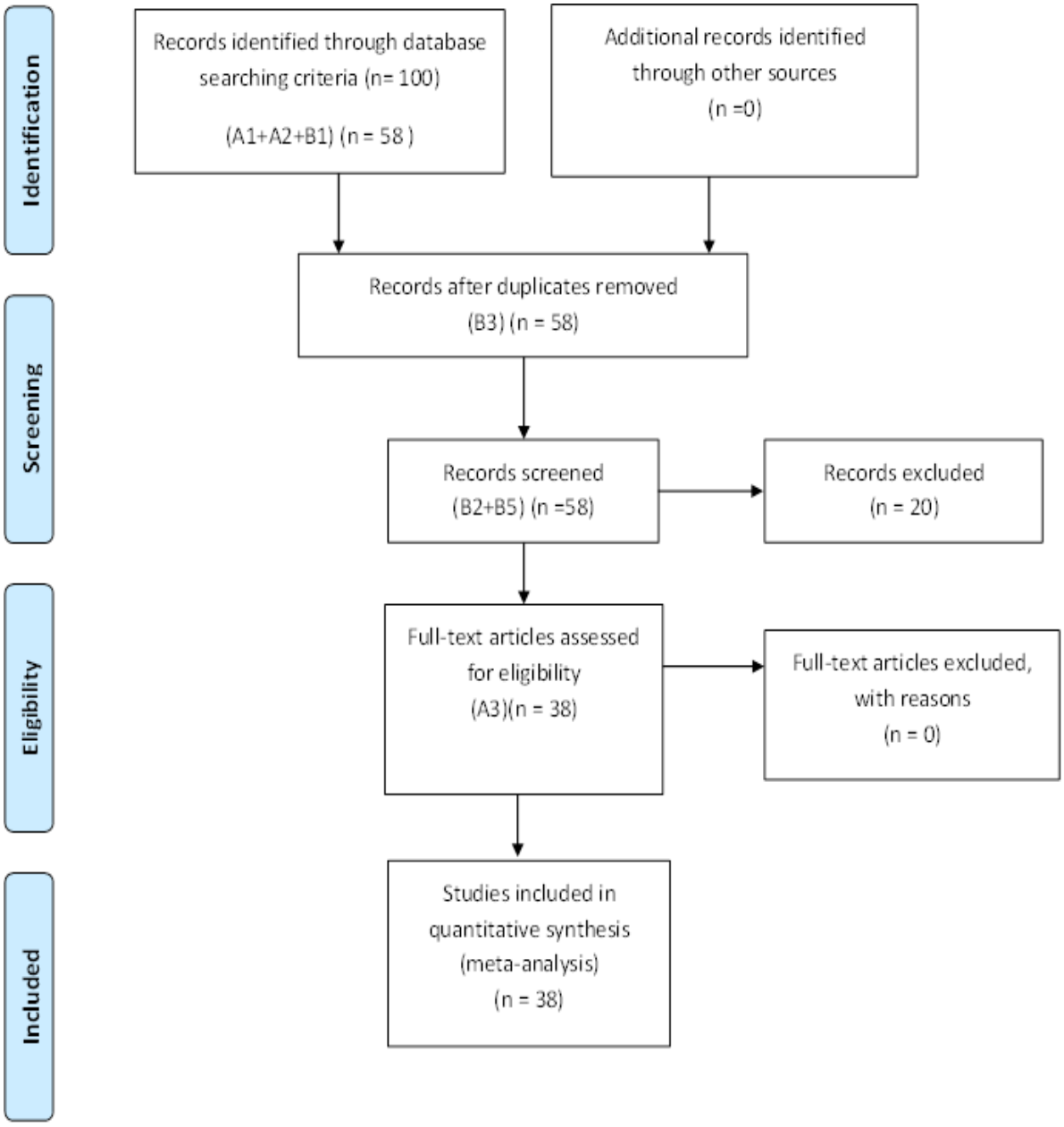

Figure 1Process for SLR Transparency Using PRISMA Flow Diagram(Moher2009.Pdf, n.d.)

2.2 SCREENING STAGE:

At this level, we implement selection criteria by going through the title, abstract, metadata and conclusions to sort out appropriate articles. 58 documents will be reviewed at this point. There are no duplicate complaints (B3), and there are no papers that are not specifically linked to detecting cryptocurrency fraud. (B5). In the qualifying step, 58 sheets were still used.

2.3 ELIGIBILITY STAGE:

This is the step of quality assurance. The research is founded on authentic published papers. All duplications were carefully verified to ensure the review's standard. usefulness of scholarly literature included in the review process. At a later point, each study article was carefully evaluated. The articles were then limited to those that used Solutions to bitcoin scam detection methods. (A3). Furthermore, 20 articles were eliminated from the research following the filtering procedure. We chose 38 pieces after evaluating each one on the aforementioned inclusion and exclusion criteria. This stage is useful to ensure that existing articles can answer our research questions.

TABLE1: INCUSION AND EXCLUSION CRITERIA

Criteria	
Inclusion	A1. The full article was written in English A2. Both Journal article and conference papers A3. Solutions contain cryptocurrency fraud detection techniques
Exclusion	B1. The article was written outside the range 2018-2022 B2. Book and white paper B3. Duplicate copies indexed in other databases B4. Literature review or overview of other paper B5. Papers not explicitly related to crypto currency fraud detection

2.4 INCLUDED STAGE:

This is typically the data extraction step, where a total of 38 papers were chosen and the following characteristics were extracted: 1) Article must be a journal paper

2) The article must be written in English.

3) The papers that were extracted were released between 2018 and 2022.

4) The article must provide Solutions for detecting bitcoin fraud

At this point, all responses to the RQ will be recorded on a previously gathered chart.

TABLE II JOURNAL DATABASE DISTRIBUTION

Database Journal	Articles
ACM	4
IEEE	14
SPRINGER	7
ELSAVIER	3
MDPI	2
RESEARCH GATE	1
ARXIV	3
MUNIN	1
SCHOLAR	1
HINDAWI	1
TAYLOR& FRANCIS	1
Total	38

3 RESULTS AND DISCUSSION

In this part, we closely examine 38 main studies from four perspectives: Deep and machine Learning method, Accuracy, dataset, and Fraud attack kinds.

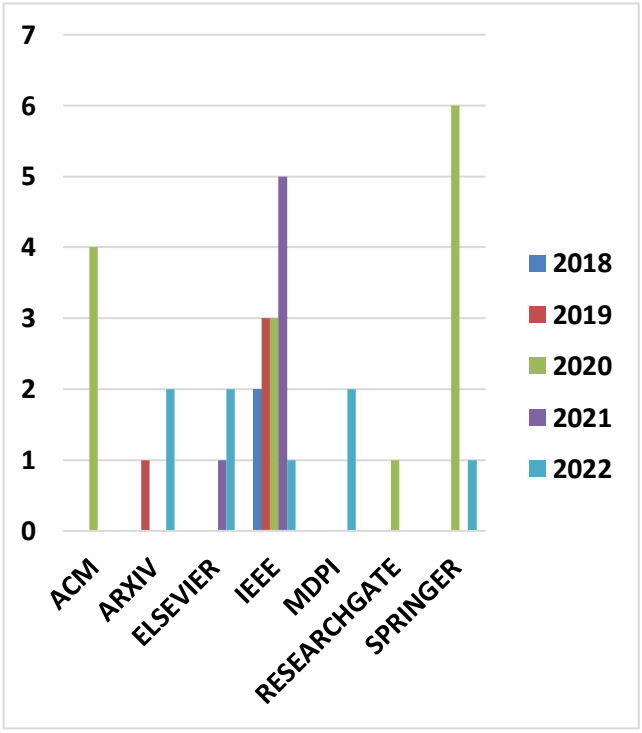

Figure 2 Total Journal articles distribution per

According to Figure 3, Cryptocurrency Fraud detection study that matches our criteria grew considerably between 2018 and 2020, declines by 2021, and is presently increasing in power. Figure 2 demonstrates that IEEE has more Journal articles than any other publication over the

span of a study period. IEEE contributed 14 articles to this evaluation, while the remaining data were shared by the other authors. Figure 4 depicts the spread of cites across some of the research articles, whereas Figure 5 depicts the bibliographical analysis network of co-citations for the chosen articles used in the report.

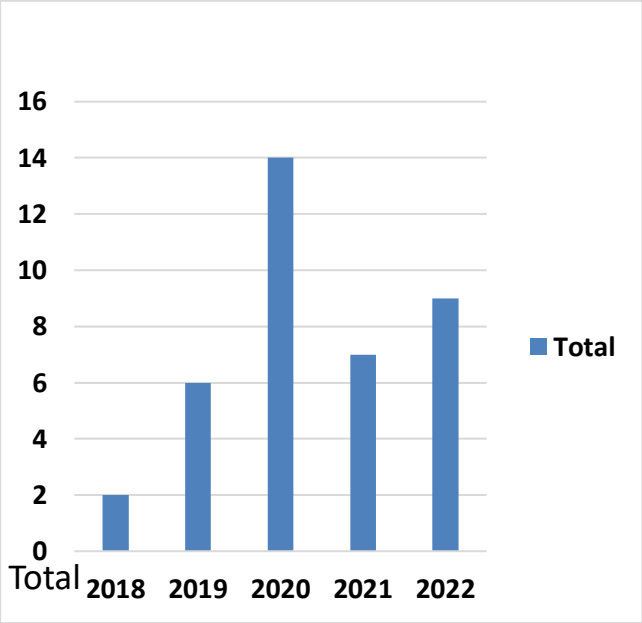

Figure 3 Total Journal articles distribution per year.

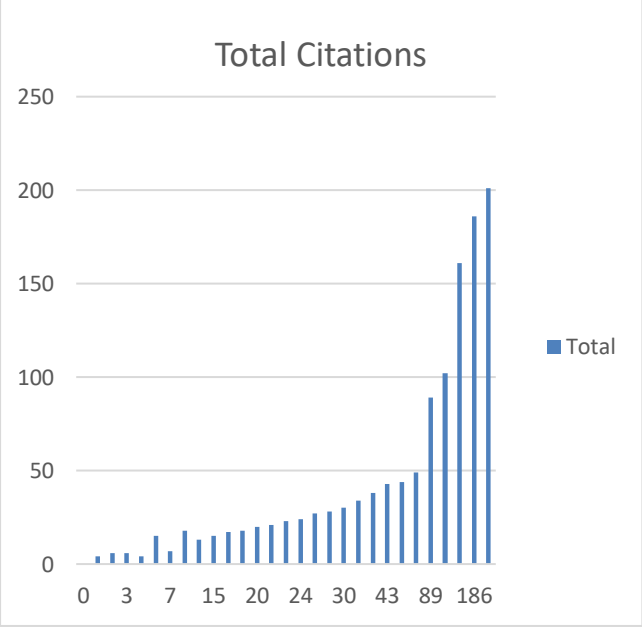

Figure 4 Frequency distribution of Citation of Articles used in the report.

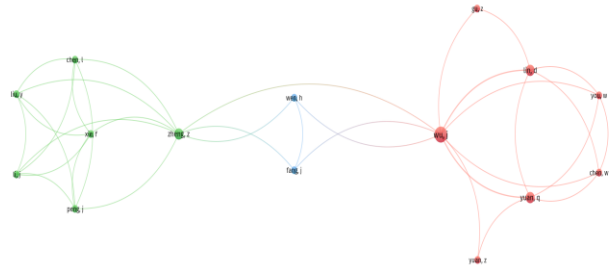

Figure 5 Bibliography analysis of co-citations for the selected articles in the report

3.1 SYSTEMATIC MAPPING OF STUDY RESULTS

RQ1 – Which is the most frequent used Techniques in Cryptocurrency fraud detection?

RQ2 – which Algorithms have been used in the research area and what are the Accuracy detection rates achieved?

We use a total of 37 available articles to answer RQ1 and 5 research articles to answer RQ2. We created a graphical and tabular cluster of literatures to describe the types of crypto fraud detection technique included in the research report as shown in Figure 6 and TABLE III respectively. It can be seen from Fig. 4 that Machine Learning Technique has the highest occurrences in our search. Figure 7 shows a graphical representation of accuracies of algorithms achieved. We bench marked accuracies from 90% and above and got the corresponding algorithms used to achieve the detection rates.

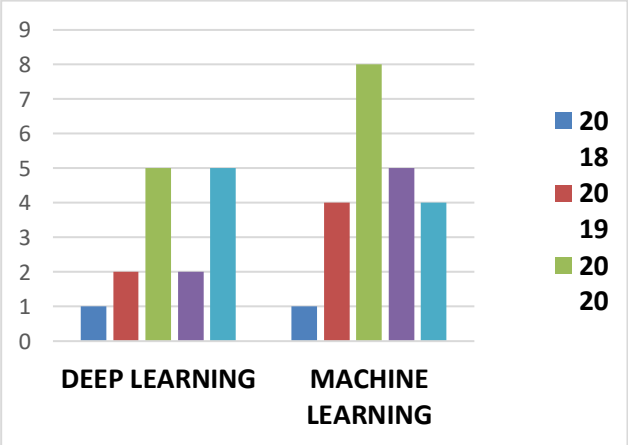

Figure 6 Cryptocurrency fraud detection Techniques frequency distribution

Deep learning approaches and machine learning approaches are the two main methods to identify bitcoin scams that can be found in the literature groups displayed in Table III. Many deep learning-based models and methods were used in deep learning approach to detect fraud. The topmost Algorithms detection models using deep learning techniques are GCN(Ismail Alarab et al., 2020), LSTM (Andreas Isnes Nilsen, 2023), and GNN (Panpan Li et al., 2023). (Ismail Alarab et al., 2020) demonstrates the skill of GCN when coupled with MultiLayer Perceptron, which is combining a feedforward neural network with a graph-based spectrum method. Their testing assessments show that, as opposed to simply applying graph convolutions to the bitcoin elliptic dataset, the combination of features generated from GCN and the hidden representation of a linear layer improves the performance of the model with an accurate detection rate of 97.4%.

(Runnan Tan et al., 2021 suggests a technique for deterring Ethereum scams by gathering transaction data that is built on Ethereum. In particular, web bots are used to collect addresses that have been flagged as fake, after which a transaction network is built using the public transaction book. Then, a network embedding method based on quantity is suggested in order to derive node characteristics for detecting fake transactions. ones are finally divided into legitimate and fake ones using the graph neural network model. The testing findings demonstrate that the system for identifying fraudulent transactions can reach an accuracy of 95%, demonstrating the system's outstanding performance in identifying fake Ethereum transactions.

(Andreas Isnes Nilsen, 2023) offers the Light Gradient Boosting Machine (LGBM) method as a method for precisely identifying fake activities. It examines different models such as Random Forest (RF), Multi-Layer Perceptron (MLP), etc., based on machine learning and soft computing algorithm for classifying Ethereum fraud detection dataset with limited attributes and compares their metrics with the LGBM approach, further optimizing the LGBM with hyper-parameter tuning; an accuracy of 99.03% was achieved. Figure 7 provides a visual summary of all the algorithms and success rates used in this study. The Machine learning approach has also shown good significant detection rates. The topmost Algorithms detection models using Machine learning techniques are LGBM (Aziz, Baluch, Patel, & Ganie, 2022)-(Aziz, Baluch, Patel, & ..., 2022), ENSEMBLE LEARNING (Alarab et al., 2020a). (Aziz, Baluch, Patel, & ..., 2022) developed a Light Gradient Boosting Machine (LGBM) technique-based model. The modified LGBM model optimized the parameters of Light GBM using the Euclidean distant structured estimation approach. The modified LGBM algorithm demonstrates a good accuracy of 99.17. The LGM approach in (Aziz, Baluch, Patel, & Ganie, 2022) uses the light gradient boosting machine (LGBM) algorithms to demonstrate the high accuracy, with 98.60% for a specific dataset scenario. Further optimizing the LGBM with hyper-parameter tuning, an accuracy of 99.03% was achieved. (Alarab et al., 2020a) used supervised learning methods for anti-money laundering in Bitcoin. An ensemble learning method is utilized using a combination of the given supervised learning models, which outperforms the given classical methods using the Elliptic data set, they are able to predict licit/illicit transactions with an accuracy of 98.13%.

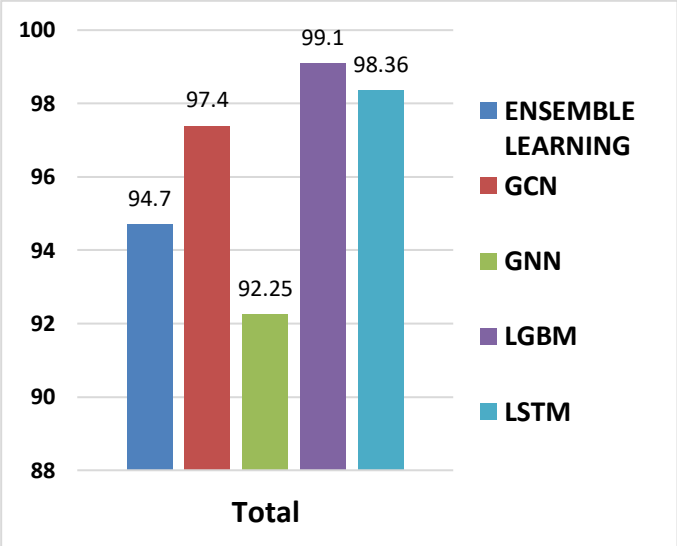

Figure 7 Algorithms and Accuracy rates

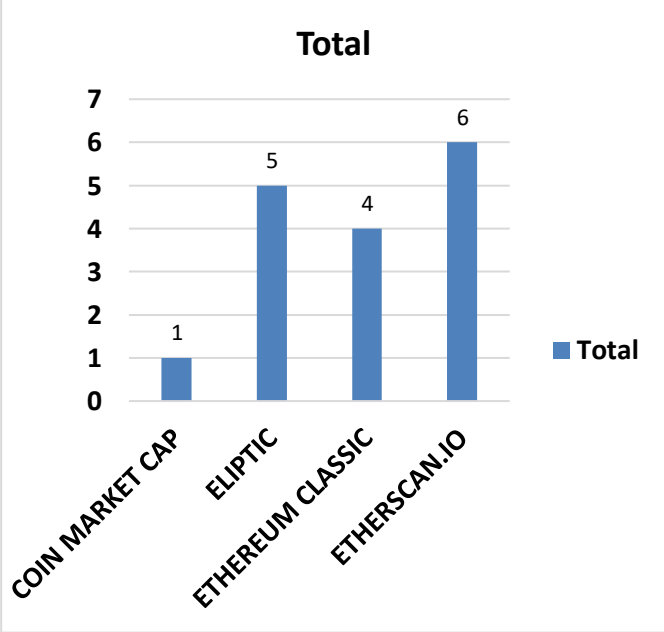

Figure 8 Frequency distribution of dataset sources used in Cryptocurrency fraud detection

TABLE III. Overview of RQ1

Analysis Type	Literature
Machine Learning	(Aziz, Baluch, Patel, & Ganie, 2022), (Baek et al., 2019), (Jung et al., 2019), (Ibrahim et al., 2021), (Kumar et al., 2020), (Poursafaei et al., 2020),(Liao et al., 2019), (Dokuz et al., 2020), (Bartoletti et al., 2018), (Lee et al., 2020), (Yin et al., 2019), (Sureshbhai et al., 2020),(B. Chen et al., 2021),(Alarab et al., 2020a),(Wu et al., 2020),(Aljofey et al., 2022),(T. Hu et al., 2021),(Wen et al., 2021),(Akba et al., 2021),(Ostapowicz & ?bikowski, 2020),(Aziz, Baluch, Patel, & ..., 2022),(Shayegan et al., 2022)
Deep Learning	(Patel et al., 2020),(Gu et al., 2022),(Liu et al., 2022),(Tan et al., 2021),(Kanezashi et al., 2022),(Singh et al., 2021),(Nan & Tao, 2018),(H. Hu et al., 2022),(Weber et al., 2019),(Li et al., 2022),(Nilsen, 2019),(Scicchitano et al., 2020),(L. Chen et al., 2020),(Alarab et al., 2020b),(Yuan et al., 2020)

RQ3 – What were the most frequently sources of dataset found in the review?

To answer this question, we use 16 articles published within the year 2018-2022 to identify the sources of the dataset used in their research and the findings to answer RQ3 is graphically represented in Figure 8. It can be seen that Elliptic, Ethereum classic and Etherscan data are the most common dataset sources used in the area of Cryptocurrency fraud detection. The Elliptic dataset are bitcoin data from(Weber et al., 2019) which contributed the Elliptic Data Set in their research, elliptic is a time series graph of over 200K Bitcoin transactions, 234K directed payment flows, and 166 node features, including ones based on non-public data; this may be the largest labelled transaction data set publicly available in any cryptocurrency.

While the Ethereum classic and Etherscan data are Ethereum dataset. They are public dataset available in Kaggle.com .The literatures that used these database sources have been summarized in TABLE IV Showing references of the articles. We bench mark a minimum of 4 articles that have used at least one category of the dataset sources mentioned above in their experiment.

TABLE IV. Overview of RQ3

S/N	Dataset type	LITERATURE
1	Eliptic	(Lorenz et al., 2020),(Singh et al., 2021),(Sureshbhai et al., 2020),(Alarab et al., 2020a),(Weber et al., 2019),
2	Etherscan	(Baek et al., 2019),(Jung et al., 2019),(Poursafaei et al., 2020),(Liao et al., 2019),(Aljofey et al., 2022),(Wen et al., 2021)
3	Ethereum Classic	(Ibrahim et al., 2021),(Kanezashi et al., 2022),(Scicchitano et al., 2020),(Aziz, Baluch, Patel, & ..., 2022)
4	Coin Market Cap	(Gu et al., 2022)

RQ4 – What were the commonly types of fraud involved with cryptocurrency

We answered this question by looking at the types of Fraud involved in the attack and the vulnerable cryptocurrency network. Smart contract fraud also known as Ponzi schemes have been used all across both the Bitcoin and Ethereum network to perform fraud. Figure 9 and Table v summarizes the RQ4 in great details both graphical and tabular references were used.

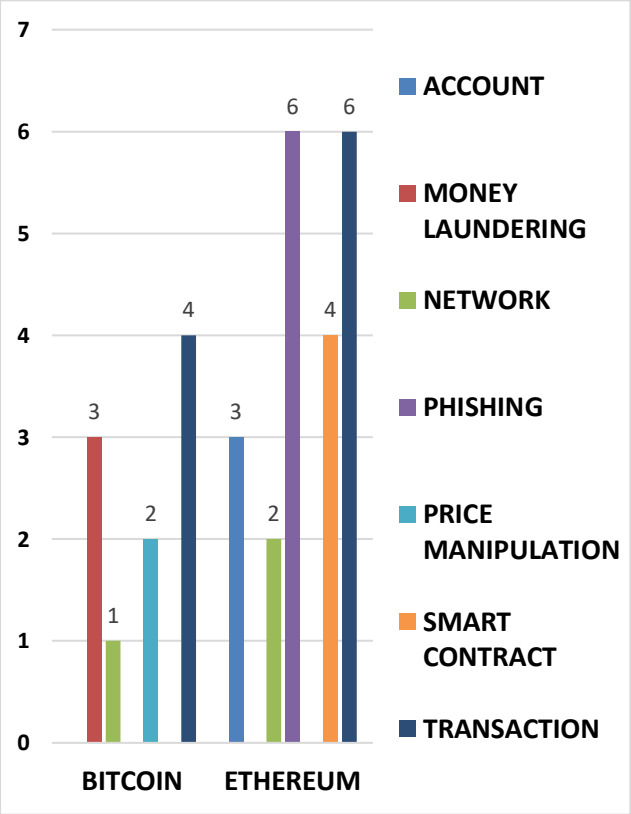

Figure 9 Frequency distribution of different Fraud attacks on the cryptocurrency network.

Table V. displays a tabular clustered reference showing the various type of fraud discussed in different research articles. It shows the most frequently form of fraud used in both the Bitcoin and Ethereum Network. From the literatures we were able to classify fraud in seven different types as shown Table V.

3.2 IDENTIFIED GAPS:

In this section, we discuss the major gaps in some areas concerning Cryptocurrency Fraud detection on the basis of three aspects that need further research and development.

A) Model Explainability: We observed in this survey paper that very high accuracies were found in the literatures but they lack explainability model considerations for black box concept of machine learning. We consider visualization for analysis and explainability, which is difficult given the size and dynamism of real-world transaction graphs(Weber et al., 2019)

B) Scarcity of labelled datasets: labels are so scarce that traditional supervised algorithms are inapplicable. Here, we address money laundering detection assuming minimal access to label datasets(Lorenz et al., 2020).

C) Un-Standardized sources of dataset : We found that a wide variety of sources of datasets are available, like marketcoincap, GitHub, own website.One of the biggest obstacles to detecting abnormal contract accounts on Ethereum is the severe data class imbalance(Aljofey et al., 2022). Two supervised methods, SVM and MLP, have zero recall with both three and nine features of the collected dataset. One of the possible reasons for this behavior is severe dataset class imbalance can skew the 0.30 decision boundaries more toward the minority class (B. Chen et al., 2021)

3.3 RECOMMENDATIONS ON FUTURE RESEACH DIRECTIONS:

In this section, we highlight various research directions for researchers in the field, which require considerable efforts to improve the performance and reliability of the cryptocurrency research domain. These research directions are presented below.

A) STANDARDIZED DATASET:

Research work is required to develop more benchmark datasets. The Standardized dataset formation can also include synthetic samples to deal with the data class imbalance problem.

B) EXPLAINABILITY MODELS INCLUSION:

Our study showed that researchers evaluated fraud detection rates in cryptocurrency. Nonetheless, a considerable number of research articles failed to evaluate the model explainabilty for real life applications especially (Patel et al., 2020),(Nilsen, 2019),(Aziz, Baluch, Patel, & Ganie, 2022),(Alarab et al., 2020b). There is need to explore Explainability AI integration in detecting fraud for real life applications.

C) LABELED DATASET CREATION:

Our study showed that the domain contains limited availability of large, high-quality datasets that have been properly labeled for use in training machine learning models

Table V: Overview of Fraud Attack Types and Literatures

S/N	FRAUD TYPE	LITERATURE
1	Account Anomalies	(Ibrahim et al., 2021),(Poursafaei et al., 2020),(Ostapowicz & ?bikowski, 2020)
2	Money Laundering	(Lorenz et al., 2020),(Alarab et al., 2020a),(Weber et al., 2019)
3	Network Anomalies	(Patel et al., 2020),(Scicchitano et al., 2020),(Alarab et al., 2020b)
4	Phishing	(Kanezashi et al., 2022),(Wu et al., 2020),(Li et al., 2022),(Wen et al., 2021),(Yuan et al., 2020),(L. Chen et al., 2020)
5	Price manipulation	(Dokuz et al., 2020),(Akba et al., 2021)
6	Smart contract (Ponzi)	(Jung et al., 2019),(Liu et al., 2022),(H. Hu et al., 2022),(Bartoletti et al., 2018),
7	Transaction Exchange Anomalies	(Aziz, Baluch, Patel, & Ganie, 2022),(Baek et al., 2019),(Gu et al., 2022),(Tan et al., 2021),(Poursafaei et al., 2020),(Nan & Tao, 2018),(Liao et al., 2019),(Lee et al., 2020),(Aziz, Baluch, Patel, & ..., 2022),(Shayegan et al., 2022)

4.0 CONCLUSION

This SLR research conducted could filter 38 papers out of 100 papers using the search criteria used in this study. In RQ1and RQ2, there were 37 articles accessed to conclude on the research question. RQ3 used 16 articles while RQ4 used a total of 31 articles. The majority of researchers are spread across a period of 2 years i.e., 2020, 2021 and 2022. We were able to identify gaps and recommend future research directions in the domain. Our results indicate that the majority of fraud in the cryptocurrency domain takes place across two cryptocurrency network which are Bitcoin and Ethereum.

REFERENCE

] Kharif, O. (2014). Mt. Gox CEO claims 850,000 bitcoins worth $480m have gone missing. Bloomberg Businessweek. Retrieved from https://www.bloomberg.com/news/articles/2014-02-28/mt-gox-ceo-says-850-000-bitcoins-worth-480 million-have-disappeared—Search. (n.d.). Retrieved January 5, 2023, from

Akba, F., Medeni, I., Guzel, M., & Askerzade, I. (2021). Manipulator Detection in Cryptocurrency Markets Based on Forecasting Anomalies. IEEE Access, Query date: 2023-01-01 12:49:58. https://ieeexplore.ieee.org/abstract/document/9502700/

Alarab, I., Prakoonwit, S., & Nacer, M. (2020a). Comparative analysis using supervised learning methods for anti-money laundering in bitcoin. … Conference on Machine Learning …, Query date: 2023-01-01 12:49:58. https://doi.org/10.1145/3409073.3409078

Alarab, I., Prakoonwit, S., & Nacer, M. (2020b). Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain. … Conference on Machine Learning …, Query date: 2023-01-01 12:49:58. https://doi.org/10.1145/3409073.3409080

Aljofey, A., Rasool, A., Jiang, Q., & Qu, Q. (2022). A Feature-Based Robust Method for Abnormal Contracts Detection in Ethereum Blockchain. Electronics, Query date: 2023-01-01 12:49:58. https://www.mdpi.com/2079-9292/11/18/2937

Andreas Isnes Nilsen. (2023). Limelight: Real-Time Detection of Pump-and-Dump Events on Cryptocurrency Exchanges Using Deep Learning.

Aziz, R., Baluch, M., Patel, S., & ... (2022). A Machine Learning based Approach to Detect the Ethereum Fraud Transactions with Limited Attributes. … International Journal of …, Query date: 2023-01-01 12:49:58. https://scholar.archive.org/work/uqv5zzlvt5f5jb5kjglm64ljtm/access/wayback/https://kijoms.uokerbala.edu.iq/cgi/viewcontent.cgi?article=3229&context=home

Aziz, R., Baluch, M., Patel, S., & Ganie, A. (2022). LGBM: a machine learning approach for Ethereum fraud detection. International Journal of …, Query date: 2023-01-01 12:49:58. https://doi.org/10.1007/s41870-022-00864-6

Baek, H., Oh, J., Kim, C., & Lee, K. (2019). A model for detecting cryptocurrency transactions with discernible purpose. … Conference on Ubiquitous and …, Query date: 2023-01-01 12:49:58. https://ieeexplore.ieee.org/abstract/document/8806126/

Bao, F., & Li, X. (2019). A survey on cryptocurrency fraud detection. International Journal of Web and Grid Services, 15(3), 199-216. (n.d.).

Bartoletti, M., Pes, B., & Serusi, S. (2018). Data mining for detecting bitcoin ponzi schemes. … Crypto Valley Conference on …, Query date: 2023-01-01 12:49:58. https://ieeexplore.ieee.org/abstract/document/8525395/

Chen, B., Wei, F., & Gu, C. (2021). Bitcoin Theft Detection Based on Supervised Machine Learning Algorithms. Security and Communication Networks, Query date: 2023-01-01 12:49:58. https://www.hindawi.com/journals/scn/2021/6643763/

Chen, L., Peng, J., Liu, Y., Li, J., Xie, F., & Zheng, Z. (2020). Phishing scams detection in ethereum transaction network. ACM Transactions on …, Query date: 2023-01-01 12:49:58. https://doi.org/10.1145/3398071

Dokuz, A., Çelik, M., & Ecemi?, A. (2020). Anomaly detection in bitcoin prices using DBSCAN Algorithm. European Journal of Science and …, Query date: 2023-01-01 12:49:58. https://www.researchgate.net/profile/Ahmet-Dokuz/publication/341052358_Anomaly_Detection_in_Bitcoin_Prices_using_DBSCAN_Algorithm/links/5eabf9a4a6fdcc70509e065b/Anomaly-Detection-in-Bitcoin-Prices-using-DBSCAN-Algorithm.pdf

Gu, Z., Lin, D., & Wu, J. (2022). On-chain analysis-based detection of abnormal transaction amount on cryptocurrency exchanges. Physica A: Statistical Mechanics and Its Applications, Query date: 2023-01-01 12:49:58. https://www.sciencedirect.com/science/article/pii/S0378437122005258

Hu, H., Bai, Q., & Xu, Y. (2022). Scsguard: Deep scam detection for ethereum smart contracts. IEEE INFOCOM 2022-IEEE Conference on …, Query date: 2023-01-01 12:49:58. https://ieeexplore.ieee.org/abstract/document/9798296/

Hu, T., Liu, X., Chen, T., Zhang, X., Huang, X., Niu, W., & ... (2021). Transaction-based classification and detection approach for Ethereum smart contract. Information Processing …, Query date: 2023-01-01 12:49:58. https://www.sciencedirect.com/science/article/pii/S0306457320309547

Ibrahim, R., Elian, A., & ... (2021). Illicit account detection in the ethereum blockchain using machine learning. … Conference on Information …, Query date: 2023-01-01 12:49:58. https://ieeexplore.ieee.org/abstract/document/9491653/

Ismail Alarab, Simant Prakoonwit, & Mohamed Ikbal Nacer. (2020). Competence of Graph Convolutional Networks for Anti-Money Laundering in Bitcoin Blockchain. Proceedings of the 2020 5th International Conference on Machine Learning Technologies. https://doi.org/10.1145/3409073.3409080

Jung, E., Tilly, M. L., Gehani, A., & ... (2019). Data mining-based ethereum fraud detection. 2019 IEEE International …, Query date: 2023-01-01 12:49:58. https://ieeexplore.ieee.org/abstract/document/8946232/

Kanezashi, H., Suzumura, T., Liu, X., & Hirofuchi, T. (2022). Ethereum Fraud Detection with Heterogeneous Graph Neural Networks. ArXiv Preprint ArXiv …, Query date: 2023-01-01 12:49:58. https://arxiv.org/abs/2203.12363

Kaur, M., & Singh, G. (2019). Cryptocurrency fraud detection using machine learning techniques: A review. In 2019 Second International Conference on Communication and Electronics Systems (ICCES) (pp. 1-5). IEEE. (n.d.).

Kshetri, N. (2018). Initial coin offerings: A review of the regulatory challenges. Journal of Financial Regulation and Compliance, 26(4), 318-333. (n.d.).

Kumar, N., Singh, A., Handa, A., & Shukla, S. (2020). Detecting malicious accounts on the Ethereum blockchain with supervised learning. … and Machine Learning, Query date: 2023-01-01 12:49:58. https://doi.org/10.1007/978-3-030-49785-9_7

Lee, C., Maharjan, S., Ko, K., & Hong, J. (2020). Toward detecting illegal transactions on bitcoin using machine-learning methods. … Conference on Blockchain and …, Query date: 2023-01-01 12:49:58. https://doi.org/10.1007/978-981-15-2777-7_42

Li, P., Xie, Y., Xu, X., Zhou, J., & Xuan, Q. (2022). Phishing Fraud Detection on Ethereum using Graph Neural Network. ArXiv Preprint ArXiv:2204.08194, Query date: 2023-01-01 12:49:58. https://arxiv.org/abs/2204.08194

Liao, J., Tsai, T., He, C., & ... (2019). Soliaudit: Smart contract vulnerability assessment based on machine learning and fuzz testing. … Systems, Management and …, Query date: 2023-01-01 12:49:58. https://ieeexplore.ieee.org/abstract/document/8939256/

Liu, L., Tsai, W., Bhuiyan, M., Peng, H., & Liu, M. (2022). Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum. Future Generation Computer …, Query date: 2023-01-01 12:49:58. https://www.sciencedirect.com/science/article/pii/S0167739X21003319

Lorenz, J., Silva, M., Aparício, D., Ascensão, J., & ... (2020). Machine learning methods to detect money laundering in the bitcoin blockchain in the presence of label scarcity. Proceedings of the First …, Query date: 2023-01-01 12:49:58. https://doi.org/10.1145/3383455.3422549

Moher2009.pdf. (n.d.).

Nan, L., & Tao, D. (2018). Bitcoin mixing detection using deep autoencoder. 2018 IEEE Third International Conference on …, Query date: 2023-01-01 12:49:58. https://ieeexplore.ieee.org/abstract/document/8411868/

Nilsen, A. (2019). Limelight: Real-time detection of pump-and-dump events on cryptocurrency exchanges using deep learning. munin.uit.no. https://munin.uit.no/handle/10037/15733

Ostapowicz, M., & ?bikowski, K. (2020). Detecting fraudulent accounts on blockchain: A supervised approach. International Conference on Web Information …, Query date: 2023-01-01 12:49:58. https://doi.org/10.1007/978-3-030-34223-4_2

Panpan Li, Yunyi Xie, & Xinyao Xu et al. (2023). Phishing Fraud Detection on Ethereum using Graph Neural Network.

Patel, V., Pan, L., & Rajasegarar, S. (2020). Graph deep learning based anomaly detection in ethereum blockchain network. International Conference on Network and …, Query date: 2023-01-01 12:49:58. https://doi.org/10.1007/978-3-030-65745-1_8

Poursafaei, F., Hamad, G., & Zilic, Z. (2020). Detecting malicious Ethereum entities via application of machine learning classification. … for Innovative Networks and …, Query date: 2023-01-01 12:49:58. https://ieeexplore.ieee.org/abstract/document/9223304/

Runnan Tan, Qingfeng Tan, & +1 author Zhao Li. (2021). Graph Neural Network for Ethereum Fraud Detection. IEEE International Conference on Big Knowledge.

Scicchitano, F., Liguori, A., Guarascio, M., Ritacco, E., & ... (2020). Deep autoencoder ensembles for anomaly detection on blockchain. … on Methodologies for …, Query date: 2023-01-01 12:49:58. https://doi.org/10.1007/978-3-030-59491-6_43

SEC. (2020). Investor Alert: Ponzi Schemes. Retrieved from https://www.sec.gov/oiea/investor-alerts-bulletins/ia_ponzi.html—Search. (n.d.). Retrieved January 5, 2023, from https://www.bing.com/search?q=SEC.+(2020).+Investor+Alert%3A+Ponzi+Schemes.+Retrieved+from+https%3A%2F%2Fwww.sec.gov%2Foiea%2Finvestor-alerts-bulletins%2Fia_ponzi.html&cvid=be4d7f806d2e45768ee59f0a311a39fe&aqs=edge..69i57.1299j0j4&FORM=ANAB01&PC=ASTS

Shayegan, M., Sabor, H., Uddin, M., & Chen, C. (2022). A Collective Anomaly Detection Technique to Detect Crypto Wallet Frauds on Bitcoin Network. Symmetry, Query date: 2023-01-01 12:49:58. https://www.mdpi.com/2073-8994/14/2/328

Singh, A., Gupta, A., Wadhwa, H., & ... (2021). Temporal Debiasing using Adversarial Loss based GNN architecture for Crypto Fraud Detection. … on Machine Learning …, Query date: 2023-01-01 12:49:58. https://ieeexplore.ieee.org/abstract/document/9680261/

Sureshbhai, P., Bhattacharya, P., & ... (2020). KaRuNa: A blockchain-based sentiment analysis framework for fraud cryptocurrency schemes. 2020 IEEE International …, Query date: 2023-01-01 12:49:58. https://ieeexplore.ieee.org/abstract/document/9145151/

Tan, R., Tan, Q., Zhang, P., & Li, Z. (2021). Graph neural network for ethereum fraud detection. 2021 IEEE International …, Query date: 2023-01-01 12:49:58. https://ieeexplore.ieee.org/abstract/document/9667674/

Wang, Z., Chen, M., & Lee, W. C. (2018). A survey on cryptocurrency fraud detection techniques. In 2018 IEEE International Conference on Big Data (Big Data) (pp. 438-447). IEEE. (n.d.).

Weber, M., Domeniconi, G., Chen, J., Weidele, D., & ... (2019). Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics. ArXiv Preprint ArXiv …, Query date: 2023-01-01 12:49:58. https://arxiv.org/abs/1908.02591

Wen, H., Fang, J., Wu, J., & Zheng, Z. (2021). Transaction-based hidden strategies against general phishing detection framework on ethereum. … Symposium on Circuits and …, Query date: 2023-01-01 12:49:58. https://ieeexplore.ieee.org/abstract/document/9401091/

Wen, Z., Zeng, D., Li, Y., Li, H., & Lu, J. (2019). Blockchain analytics: A survey. ACM Computing Surveys (CSUR), 52(1), 1-38. (n.d.).

Wu, J., Yuan, Q., Lin, D., You, W., Chen, W., & ... (2020). Who are the phishers? Phishing scam detection on ethereum via network embedding. IEEE Transactions …, Query date: 2023-01-01 12:49:58. https://ieeexplore.ieee.org/abstract/document/9184813/

Yin, H. S., Langenheldt, K., Harlev, M., & ... (2019). Regulating cryptocurrencies: A supervised machine learning approach to de-anonymizing the bitcoin blockchain. Journal of …, Query date: 2023-01-01,12:49:58. https://doi.org/10.1080/07421222.2018.1550550

Yuan, Z., Yuan, Q., & Wu, J. (2020). Phishing detection on Ethereum via learning representation of transaction subgraphs. International Conference on Blockchain and …, Query date: 2023-01-01 12:49:58. https://doi.org/10.1007/978-981-15-9213-3_14

Zohar, A. (2015). Bitcoin: Under the hood. Communications of the ACM, 58(9), 104–113. https://doi.org/10.1145/2701411