Machine Learning on Blockchain Data: A Systematic Mapping Study

Georgios Palaiokrassas[1,2], Sarah Bouraga[3], Leandros Tassiulas[1,2]

[1]Yale Institute for Network Science, Yale University, USA
[2]Department of Electrical Engineering, Yale University, USA
[3]Namur Digital Institute (NADI), Belgium
{georgios.palaiokrassas, leandros.tassiulas}@yale.edu,
sarah.bouraga@unamur.be

Abstract

Context: Blockchain technology has drawn growing attention in the literature and in practice. Blockchain technology generates considerable amounts of data and has thus been a topic of interest for Machine Learning (ML).

Objective: The objective of this paper is to provide a comprehensive review of the state of the art on machine learning applied to blockchain data. This work aims to systematically identify, analyze, and classify the literature on ML applied to blockchain data. This will allow us to discover the fields where more effort should be placed in future research.

Method: A systematic mapping study has been conducted to identify the relevant literature. Ultimately, 159 articles were selected and classified according to various dimensions, specifically, the domain use case, the blockchain, the data, and the machine learning models.

Results: The majority of the papers (49.7%) fall within the Anomaly use case. Bitcoin (47.2%) was the blockchain that drew the most attention. A dataset consisting of more than 1.000.000 data points was used by 31.4% of the papers. And Classification (46.5%) was the ML task most applied to blockchain data.

Conclusion: The results confirm that ML applied to blockchain data is a relevant and a growing topic of interest both in the literature and in practice. Nevertheless, some open challenges and gaps remain, which can lead to future research directions. Specifically, we identify novel machine learning algorithms, the lack of a standardization framework, blockchain scalability issues and cross-chain interactions as areas worth exploring in the future.

Keywords: Blockchain, Machine learning, Systematic mapping study

1 Introduction

Blockchain technology has sparked a lot of interest over the years. A particularly interesting characteristic of the technology is the transparency it offers. Indeed, all the transactions recorded on a public blockchain (amounting to hundreds of thousands of transactions a day, just for Bitcoin) can be viewed, retrieved and analyzed by anyone. This is a huge paradigm shift, compared to incumbent institutions such as traditional banks.

The amount of available blockchain data offers a lot of potential for analysis. We can analyze the blockchain data to discover unknown patterns in the data, or to predict the next cryptocurrency price, or to detect fraud to name a few. In order to carry out these types of analyses, we can use machine learning, a subfield of Artificial Intelligence. Since machine learning requires a lot of data to perform well, and since blockchain data are public and available in large quantities, this seems like a match made in heaven.

This claim is supported by the plethora of scientific articles we analyze here. Many researchers addressed the questions raised above, i.e. they tried to discover hidden patterns in blockchain data, they proposed solutions for the prediction of cryptocurrency prices, others focused on the detection of fraudulent activity on a blockchain, and multiple other use cases.

Due to the rapid evolution of both technologies (blockchain and machine learning), it is not trivial to keep track of the state of the art: What has been done? How? On which platform?... We believe it is essential for researchers and practitioners to have a clear view of the current state of the art. On the one hand, practitioners need to know the new solutions for a given problem, taking advantage of the latest advances in a given field. Researchers, on the other hand, need to know the works they can build on and the research directions they can pursue.

Hence, the aim and corresponding contribution of this paper is to propose a **Systematic Mapping Study** of scientific papers applying machine learning to blockchain data. As explained in Section 3, we apply the rigorous methodology and follow the guidelines proposed by [1, 2]. Specifically, our contribution is fourfold:

1. We **identify, analyze and organize 159 papers**, published between 2008 and 2023, applying machine learning to blockchain data. Section 4 shows the distribution of the papers across venues (Book chapter, Conference proceedings, and journal articles) and their evolution throughout the years.

2. Using keywording, we propose a **classification scheme** organizing the studies across multiple dimensions, namely: the Use Case, the Blockchain, the Data, and the Machine Learning task. We present the classification scheme in Section 5.

3. We propose a **mapping of the studies**, focusing on the use cases: Address classification, Anomaly detection, Cryptocurrency price prediction, Performance prediction, and Smart contract vulnerability detection. We present the mapping results in Section 6.

4. We identify potential **research gaps** in Section 7, where we also discuss the results of this work.

The main aim of this work is to investigate the current state of the art regarding machine learning on blockchain data. Specifically, we aim to assess the academic publication aspect, such as the popular forums and publication types; as well as the technical aspects, such as the blockchains that have been analyzed, the datasets used and/or curated by researchers, and the machine learning algorithms that were applied. We hope the study will provide the reader with a clear overview of the current research of machine learning on blockchain data, and that it will highlight potential research gaps, suggesting potential future research directions for researchers.

1.1 Related Surveys

Various authors proposed related surveys, which we classified into three categories: (i) general surveys about blockchain and machine learning, (ii) surveys about blockchain and machine learning in a specific sector/industry or application, and (iii) systematic reviews.

Some researchers proposed an overview of blockchain technology and of artificial intelligence applications in the blockchain. Siddiqui & Haroon [3] introduced blockchain technology, its characteristics and benefits; then explored how AI and blockchain can be combined in order to mitigate their limitations. The authors also offered a wide range of examples of applications of these two technologies; and discussed the case of edge computing. Similarly, Inbaraj & Chaitanya [4] provided an overview of blockchain and AI, discussed the implementation of blockchain in various industries, and discussed the integration of blockchain and AI in various applications.

Other works focused on blockchain and artificial intelligence in a specific sector or for a specific application. A number of authors proposed an analysis of existing works addressing blockchain and machine learning related to the Internet of Things (IoT). Aoun et al. [5] proposed an overview of IoT, its challenges and how blockchain technology can help in the development of the Industry 4.0. In [6], the authors provided a summary and analysis of such works using three perspectives, namely: consensus mechanism, storage, and communication. The authors discussed how blockchain and machine learning interact in Industrial IoT (IIoT) and highlight the security and privacy risks of such solutions. Liu et al. [7] analyzed works exploring blockchain-enabled federated learning in the context of Digital Twin, from aspects pertaining to security, fault-tolerance, fairness, efficiency, cost-saving, profitability, and support for heterogeneity. Various authors addressed the issue of IoT security. On the one hand, Williams et al. [8] reviewed the security in IoT and emphasized the impact of emerging technologies, including fog/edge/cloud computing and quantum computing in addition to blockchain and machine learning. On the other hand, in [9], the authors analyzed how machine learning, artificial intelligence, and blockchain technology can help to address IoT security. In [10], the authors discussed how we can integrate blockchain technology and artificial intelligence with smart grids in order to facilitate prosumers' participation in energy markets.

Han et al. [11] adopted the same approach but applied it to the case of accounting and auditing. Cheng et al. [12] reported on the use of machine learning and blockchain technology in the healthcare sector, and more specifically discussed the implications for cancer care.

A study closer to our research here would be [13], where the authors analyzed works related to cryptocurrency research and machine learning. The findings of this work: (i) confirm the popularity of the topic in research; (ii) show that cryptocurrency price (or related) prediction is the most popular topic; and (iii) indicate that many different algorithms are used and that common problems such as overfitting and interpretability are still present.

Mainly two elements differentiate our work here from these related surveys. Firstly, we do not focus on a specific area, but provide an overview of existing works pertaining to a wide range of industries, sectors, and applications. In particular, we do not restrict our analysis to cryptocurrency as in [13] but our review encompasses works related to a wide range of use cases. Secondly, we focus on machine learning on blockchain data; while many of the mentioned surveys addressed works about the integration of the two technologies to a specific problem or opportunity.

Finally, we identified a bibliometric analysis, two systematic reviews, and a survey. Bai & Sarkis [14] conducted a bibliometric and network analysis to identify research areas related to formal analytical modeling for blockchain in the domain of supply chains. In [15], the authors performed a systematic review of the use of blockchain management and machine learning in the particular context of IoT environment. Lin et al. [16] carried out a systematic review and analyzed 25 papers treating unsupervised learning, supervised learning and topological analysis for the detection of illicit transactions on the Bitcoin blockchain. Finally, a comprehensive survey was conducted in [17], where the authors depicted the state of the art regarding anomaly detection in blockchain networks. They analyzed papers and classified them based on the blockchain layers, namely, the data layer, the network layer, the incentive layer, and the smart contract layer.

We believe our work is different from the mentioned surveys and hence adds value to the literature. Indeed, the scope we consider here is broader than the ones addressed in [14, 15, 16, 17]. We propose a coarse-grained analysis of the state of the art regarding machine learning applied to blockchain data. We do not focus here on a particular use case or industry. In addition, conducting our review now allows us to consider recently published papers that could not have been treated by the previous surveys. Finally, for the coarse-grained analysis, we propose different classification dimensions than the ones discussed in previous surveys. The current work complements thus the existing surveys proposed by fellow researchers.

2 Background

As stated above, the availability of large volumes of blockchain data offers a great opportunity for analysis. Classical machine learning tasks - such as hidden patterns, trends, or outliers detection - can be performed on these data. In the following subsections, we offer a background on blockchain technology and on machine learning.

2.1 Blockchain

Blockchain was originally proposed in 2008 as the accounting method for Bitcoin cryptocurrency [18]. The technology and ideas evolved in the years that followed and many blockchains and altcoins were introduced. A milestone for the course of blockchain technology was the introduction of Ethereum in 2015 [19], an open decentralized blockchain platform which provides a virtual computing environment called Ethereum Virtual Machine, but also a Turing complete programming language to write smart contracts. Ethereum smart contracts are actually program instances running on the decentralized network and any user is allowed to deploy smart contracts enabling the development of different Decentralized Applications (DApps) with potential for different fields such as IoT [20], copyright management [21], supply chain management [22], healthcare [23], energy [24], Decentralized Finance (DeFi) [25] and many more.

Blockchain is actually a distributed ledger or distributed database recording digital transactions between two parties without the need for Third Trusted Parties (TTP). This allows the interaction of users without an intermediary, while anonymity is preserved, as one of the key blockchain's features. Every participating node in this peer-to-peer network has an actual "copy" of all the transactions that took place, ensuring their immutability and enhancing security. Security is also preserved by the utilization of cryptography, which is one of the principal aspects of blockchain technology.

The transactions within a ledger are verified by multiple nodes or "validators," within the cryptocurrency's peer-to-peer network using one of many varied consensus algorithms for resolving the problem of reliability in a network involving multiple unreliable nodes. Different consensus mechanisms have been proposed allowing the network of nodes to agree on the state of a blockchain. The most widely used consensus algorithms are the Proof of Work (PoW) algorithm and the Proof of Stake (PoS) algorithm [26]. Bitcoin for example uses a PoW-based consensus protocol, while Ethereum transitioned from a PoW to PoS-based consensus protocol. However, there are also other consensus algorithms, which utilize alternative implementations of PoW and PoS, as well as other hybrid implementations and some altogether new consensus strategies.

An increasing amount of blockchain data is generated through various interactions and activities. The type of data varies depending on the type of blockchains, the supported functionalities and remains unchanged given the immutable nature of ledgers. Blockchain data consists mainly of transaction and block data, smart contract logs, events, and interactions, network activity, and topology, while data analysis and machine learning techniques have been applied to them combining often external datasets such as cryptocurrency prices, news feed and public sentiment.

2.2 Machine Learning

As stated by M. Jordan and T. Mitchell, Machine Learning addresses the question of how to build computers that improve automatically through experience. It is one of today's most rapidly growing technical fields, lying at the intersection of computer science and statistics, and at the core of artificial intelligence and data science [27]. According to another definition by Deisenroth et al. [28], Machine learning is about designing algorithms that automatically extract valuable information from data with emphasis on "automatic", i.e., machine learning is concerned about general-purpose methodologies that can be applied to many datasets, while producing something that is meaningful.

A learning problem can be defined as the problem of improving some measure of performance when executing some task, through some type of training experience. For example, in our study we identified several works attempting to learn to detect fraud in blockchain transactions, where the task is to assign a label of "fraud" or "not fraud" to any given blockchain transaction. The performance metric to be improved might be the accuracy of this fraud classifier, and the training experience might consist of a collection of historical transactions, each labeled in retrospect as fraudulent or not.

A typical workflow of an ML framework commonly consists of the training phase and the testing phase, while sometimes the validation phase is part of the flow [29]. It could be noted that other steps are involved in some other categories of tasks and methods such as Reinforcement Learning or Federated Learning. In general, ML techniques can be classified into four different areas:

(i) Supervised learning where the learning algorithm learns from labeled data. The training data take the form of a collection of (x, y) pairs and the goal is to produce a prediction y* in response to a query x*,

(ii) Unsupervised learning generally involves the analysis of unlabeled data under assumptions about structural properties of the data.

(iii) Semi-supervised learning is the branch of machine learning concerned with using labeled as well as unlabeled data to perform certain learning tasks. Conceptually situated between supervised and unsupervised learning, it permits harnessing the large amounts of unlabeled data available in many use cases in combination with typically smaller sets of labeled data [30].

(iv) Reinforcement learning where the information available in the training data is intermediate between supervised and unsupervised learning. Instead of training examples that indicate the correct output for a given input, the training data in reinforcement learning are assumed to provide only an indication as to whether an action is correct or not.

Regardless of the area or the task, there are some steps appearing in the workflows of the different ML solutions and research efforts. The most common ones are: i) Data Collection; (ii) Data Preprocessing; (iii) Feature Extraction and (iv) Algorithm Selection.

3 Methodology

Following [31], we conducted this systematic mapping study by considering both the guidelines proposed by [2] and by [1]. In this section, we detail the steps we performed in order to carry out our study.

3.1 The Research Questions

Systematic mapping studies, in general, aim to provide an overview of the current research in a given area [2]. In this study, we focus on blockchain and machine learning; and we offer a coarse-grained analysis of the current research, we identify the quantity and type of research, and the gaps and future research directions. Specifically, the overarching goal can be defined by the following research questions:

- **RQ1.** Which topics related to machine learning on blockchain have been investigated and to what extent?
- **RQ2.** What diverse types of blockchain data have been analyzed and to what extent has each type been represented?
- **RQ3.** Which machine learning types of models have been applied on blockchain data and to what extent has each type of model been represented?
- **RQ4.** In which forums has research on machine learning on blockchain been published?

Answering these research questions will give us a comprehensive overview of the current state of research, and thereby addressing the main goal of this paper.

3.2 Data Sources and Search Strategy

The database sources that have been used as primary sources in this study are the following:

- **Google Scholar**: `https://scholar.google.com`
- **Springer**: `https://link.springer.com`
- **ScienceDirect**: `https://www.sciencedirect.com`

These are some of the most commonly used database sources in software engineering. We started the study in December 2022 and, given the relative novelty of the technology, we decided to search publications without any period limitation.

The first step was to define search keywords as recommended by [1]. We considered the terms “Blockchain”, “Smart contract”, “Decentralized application”, “Bitcoin”, “Ethereum”, “Machine learning”, “Analytics”, and “Artificial intelligence” as our keywords. We used the logical operators OR and AND to link the main keywords. For some database sources, we conducted several searches to cover all keywords. Specifically, we started for instance with (Blockchain AND “Machine learning”), retrieved the returned publications, and repeated the search with the other keywords combinations. For other database sources, we used the following single search string:

- ALL((blockchain or “DApp” or ”Ethereum” or “Bitcoin” or “smart contract” or ”decentralized application”) AND (“machine learning” or “analytics” or ”artificial intelligence” or ”ai”))

The search strings were applied to search the database sources by considering the title, abstract and keywords.

3.3 Study Selection

We developed inclusion and exclusion criteria in order to select the most relevant and important publications. We confronted the title, abstract and full text of the articles previously retrieved, in order to ensure that the publications fit the scope of our study.

We excluded studies that exclusively provided a discussion or a conceptual solution of blockchain and machine learning (as in [32, 33, 34, 35]). The reason for this exclusion is that we are interested in the data and models used to address a specific problem. Secondly, we are interested in the application of machine learning on blockchain data. Hence, the papers addressing the use of blockchain technology to enhance the performance of machine learning were not included (such as [36, 37]). Similarly, publications analyzing data without any features pertaining to blockchain data were excluded, for instance cryptocurrency price prediction that only use data about the historical prices (as in [38, 39, 40, 41, 42, 43, 44]) or that only use traffic data [45, 46]. Furthermore, articles where no machine learning model was applied to the data were also excluded, for instance articles providing a descriptive statistics analysis (such as [47, 48]). Finally, surveys were also excluded since they do not provide a new machine learning solution but discuss and analyze existing ones [13, 3, 4].

To summarize, the inclusion and exclusion criteria applied in this study are the following.

The inclusion criteria:

- Articles must report on the application of machine learning to blockchain data
- Articles must be peer-reviewed
- Articles must be written in English
- Articles are published in or after 2008
- Articles must be published

The exclusion criteria:

- Articles propose a discussion or a conceptual solution of blockchain and machine learning, such as surveys
- Articles are not written in English
- Articles are not peer-reviewed
- Articles are published before 2008
- Articles are on pre-press

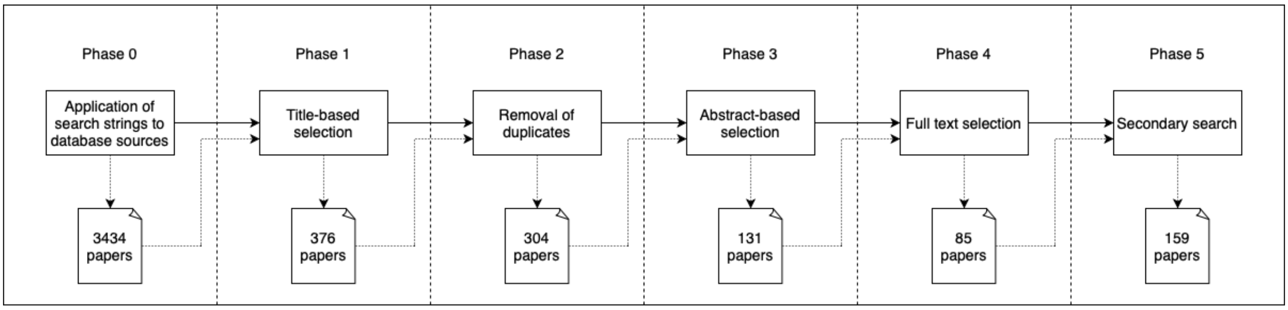

Figure 1: Selection Process

The selection of the primary studies was done in four phases and was conducted by two reviewers who examined all the retrieved studies. For each study, there was a data extractor. The data extraction form was then checked by the other reviewer. If any conflicts were raised, the authors resolved them by examining the paper together. The four phases of the selection are the following:

1. **Phase 0. Application of search strings to database sources** - *Number of papers included in the next phase: 3434.* The total number of articles retrieved from the database sources (Springer, ScienceDirect and Google Scholar) was 3434. The results of these articles were included in the next phase.

2. **Phase 1. Title-based selection.** - *Number of papers included in the next phase: 376.* In this phase, we read and assessed the paper's title using our inclusion and exclusion criteria. If the paper fit the scope of the study, it was included in the next phase. Otherwise, it was discarded. When the evaluation of the title was difficult and/or led to debate, we decided to include the paper in the next phase.

3. **Phase 2. Removal of duplicates.** - *Number of papers included in the next phase: 304.* We found 72 duplicates, we removed them from our data and we included the remaining 304 papers in the next phase.

4. **Phase 3. Abstract-based selection.** - *Number of papers included in the next phase: 131.* We read the abstract and keywords of each paper. It allowed us to confirm or infirm their selection and inclusion in the next phase. We discarded 173 papers in this phase and included the remaining 131 in the next phase.

5. **Phase 4. Full text selection.** - *Number of papers included in the next phase: 85.* In this phase, we read the full text of the 131 selected papers from phase 3. This allowed us to make the final selection and make sure that the articles included in the study were actually related to the study. Using our inclusion and exclusion criteria, we further discarded 46 articles. This resulted in a final set of primary studies consisting of 86 articles. We recorded the basic information of each of these papers in an Excel sheet, namely: the title, the authors, the publication type and the year of publication.

6. **Phase 5. Secondary search.** - *Number of papers included: 159.* In this phase, we conducted an additional selection of papers based on the references of the articles included in Phase 4. This allowed us to include papers that we may have missed in earlier phases. We proceeded in the same way as above. Specifically, we first selected the papers based on the title, and we removed the duplicates. We then read the abstract, the keywords, and the full text. In order to be included in the final set of studies, the papers had to satisfy the inclusion and exclusion criteria. This phase allowed us to include 74 additional papers, which resulted in a final set of studies consisting of 159 articles.

This process is summarized in Figure 1.

4 Studies

The studies selected in this systematic mapping study consisted of 159 articles taking the form of journal articles, conference proceedings, book chapters and workshop proceedings from 2015 to 2023. In order to address RQ4, we identified the publication years and forums of the studies. Tables 4 and 2 show a summary of the publication forums of the studies, and the distribution of the studies by publication type respectively. We can see that the *IEEE Access*, *Expert Systems with Applications*, and the *International Conference on Blockchain and Trustworthy Systems* are the most popular forums; and that 2022 and 2021 were the years where most research publications were proposed.

Publication Source	Count of papers

Book chapter	1
Blockchain Intelligence	1
Conference proceedings	82
International Conference on Blockchain and Trustworthy Systems	7
International Conference on Network and System Security	3
Hawaii International Conference on System Sciences	2
IEEE International Conference on Blockchain	2
IEEE International Conference on Blockchain and Cryptocurrency (ICBC)	2
IEEE International Symposium on Circuits and Systems (ISCAS)	2
International Conference on Complex Networks and Their Applications	2
ACM International Conference on AI in Finance (ICAIF)	1
ACSAC: Annual Computer Security Applications Conference	1
Advances in Knowledge Discovery and Data Mining	1
Biometric and surveillance technology for human and activity identification XII	1
Blockchain and Trustworthy Systems	1
Blockchain Research and Applications for Innovative Networks and Services (BRAINS)	1
CAAI International Conference on Artificial Intelligence	1
Crypto Valley Conference on Blockchain Technology (CVCBT)	1
IEEE Annual Computers, Software, and Applications Conference (COMPSAC)	1
IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social IEEE Global Communications Conference	1
IEEE Global Engineering Education Conference	1
IEEE Int Conf on High Performance Computing & Communications; Int Conf on Data Science & Systems; Int Conf on Smart City; Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys)	1
IEEE International Conference on Big Data (Big Data)	1
IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)	1
IEEE International Conference on Machine Learning and Applications	1
IEEE International Conference on Software Quality, Reliability and Security	1
IEEE Symposium Series on Computational Intelligence	1
Information Science and Applications	1
Information Security for South Africa	1
Information Systems in a Changing Economy and Society	1
Intelligent Computing and Innovation on Data Science	1
International AAAI Conference on Web and Social Media	1
International Conference of Smart Systems and Emerging Technologies (SMARTTECH)	1
International Conference on Advanced Communication Technology	1
International Conference on Advanced Data Mining and Applications	1
International Conference on Advances in Cyber Security	1
International Conference on Algorithms and Architectures for Parallel Processing	1
International Conference on Automated Software Engineering	1
International Conference on Big Data, Information and Computer Network (BDICN)	1
International Conference on Big Data and Security	1
International Conference on Blockchain Computing and Applications (BCCA)	1
International Conference on Computer Communication and Networks	1
International Conference on Computer Theory and Applications (ICCTA)	1
International Conference on Data Mining Workshops	1
International Conference on Data Science and Computer Application (ICDSCA)	1
International Conference on Deep Learning, Big Data and Blockchain	1
International Conference on Digital Forensics	1
International Conference on Information Security Theory and Practice	1
International Conference on Information Technology (ICIT)	1
International Conference on Information Technology and Quantitative Management	1
International Conference on Intelligence and Security Informatics	1
International Conference on Internet of Things: Systems, Management and Security	1
International Conference on Internet Measurement	1
International Conference on Machine Learning Technologies (ICMLT)	1
International Conference on Mobile Ad Hoc and Smart Systems (MASS)	1

International Conference on Mobile Networks and Management	1
International Conference on Parallel, Distributed, and Network-Based Processing	1
International Conference on Privacy, Security and Trust	1
International Conference on Service-Oriented System Engineering	1
International Conference on Smart City Applications	1
International Conference on Soft Computing Models in Industrial and Environmental Applications (SOCO)	1
International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)	1
International Conference on Ubiquitous and Future Networks (ICUFN)	1
International Conference Web Information Systems Engineering	1
International Congress on Blockchain and Applications	1
International Joint Conference on Neural Networks	1
International Symposium on Software Reliability Engineering	1
Italian Conference on CyberSecurity	1
Pacific-Asia Conference on Advances in Knowledge Discovery and Data Mining	1
Recent Trends in Analysis of Images, Social Networks and Texts	1
World Wide Web Conference	1
Journal	73
IEEE Access	5
Expert Systems with Applications	4
MDPI Sensors	3
Applied Soft Computing	2
Blockchain: Research and Applications	2
IEEE Transactions on Computational Social Systems	2
IEEE Transactions on Systems, Man, and Cybernetics: Systems	2
IEEE Transactions on Network Science and Engineering	2
Information Processing and Management	2
Mathematics	2
MDPI Electronics	2
PloS one	2
Academy of Accounting and Financial Studies Journal	1
ACM SIGMETRICS Performance Evaluation Review	1
ACM Transactions on Internet Technology	1
Applied Intelligence	1
CCF Transactions on Pervasive Computing and Interaction	1
Computational Economics	1
Computer Communications	1
Computer Networks	1
Data & Knowledge Engineering	1
Data Science and Management	1
Decision Support Systems	1
EPJ Data Science	1
Eurasian Economic Review	1
Finance Research Letters	1
Future Generation Computer Systems	1
IEEE Systems Journal	1
IEEE Transactions on Circuits and Systems II: Express Briefs	1
IEEE Transactions on Dependable and Secure Computing	1
IEEE Transactions on Information Forensics and Security	1
International Journal of Information Technology	1
International Journal of Forecasting	1
International Journal of Information Security	1
IOP SciNotes	1
Journal of Behavioral and Experimental Finance	1
Journal of Combinatorial Optimization	1
Journal of Computational and Applied Mathematics	1
Journal of Finance and Data Science	1
Journal of Management Information Systems	1
Journal of Risk and Financial Management	1
Journal of Supercomputing	1

Journal of Systems Architecture	1
Knowledge-Based Systems	1
Measurement: Sensors	1
Multimedia Tools and Applications	1
Neural computing and applications	1
Neural Processing Letters	1
North American Journal of Economics and Finance	1
Pattern Recognition Letters	1
Peer-to-Peer Networking and Applications	1
Physica A	1
Science China Information Sciences	1
Security and Communication Networks	1
SN Computer Science	1
Workshop proceedings	3
International Workshop on Emerging Trends in Software Engineering for Blockchain	1
International Workhsop on Financial Cryptography and Data Security	1
International Workshops of ECML PKDD on Machine Learning and Principles and Practice of Knowledge Discovery in Databases	1
Total	159

Table 1: Publication Forums of Primary Studies

Table 2: Distribution of Studies by Publication Type.

Publication Type	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**	**Total**
Book Chapter	0	0	0	0	0	0	0	0	1	0	0	1
Conference Proceedings	1	0	4	2	3	12	14	17	19	9	1	82
Journal	0	0	1	0	2	3	6	13	16	26	6	73
Workshop Proceedings	0	0	0	0	1	0	1	0	0	1	0	3
Total	1	0	5	2	6	15	21	30	36	36	7	159

5 Classification Scheme and Distribution Trend

Following [2], we designed our classification scheme by keywording. Specifically, we identified relevant keywords by reading abstract and this set of keywords allowed us to define a number of dimensions that we grouped into high level categories in order to form a structured framework. We should note that the list of keywords evolved with our reading, i.e. new keywords were added to the list as we analyzed new publications.

The studies were classified from four perspectives: (i) use case, (ii) blockchain, (iii) data, and (iv) machine learning. We should note that it is common to classify studies in software engineering based on the contribution type and the research type [2]. However, given the focus of this study, we elected not to use these dimensions. Indeed, we selected papers applying machine learning to blockchain data in order to fulfill a particular goal. Hence, most studies provide a "Method" contribution (Contribution type) and propose a "Solution" (Research type). We believe that incorporating these dimensions in our analysis would not have given the reader a lot of valuable insight.

With the classification scheme clearly defined, we sorted the relevant articles into this scheme. We used an Excel table to document the data extraction process. The table contained each category of the classification scheme. As mentioned earlier, only one reviewer filled the data extraction form (i.e. a row in our Excel table) and the other reviewer checked the form afterwards. Conflicts were resolved by analyzing and discussing the paper together. Once all conflicts were resolved, we computed the frequencies of publications for each category.

5.1 Use Case and Distribution

Using the keywording technique described in [2], we identified five major use cases:

- **Address Classification**. While pseudo-anonymity is a major property of blockchains, studies have addressed the de-anonymization of blockchain users. This use case pertains to user identification, address classification, address clustering, etc.

- **Anomaly Detection**. This use case relates to the detection of any suspicious behavior on a blockchain, e.g. Ponzi Scheme detection, Illicit transaction detection, Attack detection, etc.
- **Cryptocurrency Price Prediction**. This use case pertains to the prediction of cryptocurrency price, e.g. Bitcoin, Ether, etc.
- **Performance Prediction**. Scalability is an important challenge for the blockchain community. This use case pertains to the prediction of performance, such as the prediction of: transaction throughput, transaction confirmation time, transaction fees, etc.
- **Smart Contract Vulnerability Detection**. Given the immutability property of blockchains, vulnerability in smart contracts and DApps can have significant and dangerous consequences. Hence, studies have addressed the evaluation and detection of vulnerability in smart contracts.

Table 3 shows a summary of the distribution of the selected studies by use case.

Table 3: Distribution of Studies by Use Case.

Use Case	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
Address Classification	1	0	1	0	2	9	4	3	4	4	0	28
Anomaly Detection	0	0	1	2	1	2	8	17	22	20	6	79
Price Prediction	0	0	3	0	1	4	5	5	4	7	1	30
Performance Prediction	0	0	0	0	0	0	1	1	3	2	0	7
Vulnerability Detection	0	0	0	0	0	0	3	4	3	2	0	12
Other	0	0	0	0	2	0	0	0	0	1	0	3
Total	1	0	5	2	6	15	21	30	36	36	7	159

5.2 Blockchain and Distribution

The studies applied machine learning to data generated by various blockchains:

- **Bitcoin**. The blockchain data analyzed in the paper were coming solely from the Bitcoin blockchain.
- **Ethereum**. The blockchain data analyzed in the paper were coming solely from the Ethereum blockchain.
- **Bitcoin and Ethereum**. The blockchain data analyzed in the paper were coming from both the Bitcoin and Ethereum blockchain.
- **Multiple**. The blockchain data analyzed in the paper were coming from multiple blockchains (other than the combination of Bitcoin and Ethereum).

Table 4 shows a summary of the distribution of the selected studies by blockchain.

Table 4: Distribution of Studies by Blockchain.

Blockchain	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
Bitcoin	1	0	5	2	4	13	12	13	11	12	2	75
Ethereum	0	0	0	0	1	1	9	16	17	19	5	68
Bitcoin and Ethereum	0	0	0	0	0	0	0	1	3	2	0	6
Multiple	0	0	0	0	0	0	0	0	2	1	0	3
Other	0	0	0	0	1	1	0	0	3	2	0	7
Total	1	0	5	2	6	15	21	30	36	36	7	159

5.3 Data and Distribution

The studies in this paper used different data sources:

- **Blockchain**. The authors extracted the data directly from the blockchain they studied, whether it is Bitcoin or Ethereum.
- **Website**. The authors extracted the data from a blockchain explorer website, such as `blockchain.com`, `etherscan.io`, `walletexplorer.com`, or `xblock.pro`.

- **Published Dataset**. The authors used a public dataset made available on a popular platform such as Kaggle, or made available through another type of data repository.
- **Multiple**. The authors used various sources to construct a new dataset.

The datasets also consisted of a wide range of data points. We created the following ranges of data points:

- **< 1,000**. The dataset consists of less than 1,000 data points.
- **1,000-2,000**. The dataset consists of more than 1,000 data points but less than 2,000 data points.
- **2,000-5,000**. The dataset consists of more than 2,000 data points but less than 5,000 data points.
- **5,000-10,000**. The dataset consists of more than 5,000 data points but less than 10,000 data points.
- **10,000-50,000**. The dataset consists of more than 10,000 data points but less than 50,000 data points.
- **50,000-100,000**. The dataset consists of more than 50,000 data points but less than 100,000 data points.
- **100,000-500,000**. The dataset consists of more than 100,000 data points but less than 500,000 data points.
- **500,000-1,000,000**. The dataset consists of more than 500,000 data points but less than 1,000,000 data points.
- **> 1,000,000**. The dataset consists of more than 1,000,000 data points.

Finally, we also recorded the availability of the dataset, i.e. whether or not the authors made the data used in their study available:

- **Yes**. The authors published or provided a link to the dataset they created and used for their studies.
- **Yes (ext)**. The dataset was already public. Hence, the dataset is (already) available.
- **Upon request**. The authors added a statement in their study regarding the availability of their dataset following a (sometimes reasonable) request.
- **Partially**. A part of the dataset is available. It can happen when the authors take advantage of a public dataset and augment it with their own features.
- **No**. The authors did not mention in their paper - whether in the core of the text, in a footnote or in a statement at the end of the article - that the dataset was available. When no such indication was mentioned, we considered that the data were not available.

Tables 5 to 7 show a summary of the distribution of the selected studies by data.

Table 5: Distribution of Studies by Data Sources.

Data Source	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**	**Total**
Bitcoin	0	0	1	0	0	1	1	1	0	1	1	6
Blockchain.com	0	0	2	0	2	3	2	1	2	1	0	13
Ethereum	0	0	0	0	0	0	2	2	0	0	0	4
Etherscan.io	0	0	0	0	1	1	3	5	5	6	2	23
Walletexplorer.com	0	0	0	0	0	1	2	1	1	0	0	5
XBlock.pro	0	0	0	0	0	0	0	1	0	1	0	2
Public Dataset	0	0	1	1	0	1	3	5	9	7	0	27
Multiple	1	0	0	0	1	5	5	9	12	11	3	47
Other	0	0	1	0	0	3	2	4	3	6	1	20
Unclear	0	0	0	1	2	0	1	1	4	3	0	12
Total	1	0	5	2	6	15	21	30	36	36	7	159

Table 6: Distribution of Studies by Number of Data Points.

Data Points	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
< 1,000	0	0	0	0	1	0	0	0	1	1	0	3
1,000-2,000	0	0	0	0	2	0	0	1	1	2	0	6
2,000-5,000	0	0	0	0	0	0	1	3	4	1	0	9
5,000-10,000	0	0	0	0	0	1	2	0	3	0	3	9
10,000-50,000	0	0	0	0	0	0	3	4	3	5	1	16
50,000-100,000	0	0	0	0	1	0	1	0	3	3	0	8
100,000-500,000	0	0	0	0	0	3	1	3	7	5	1	20
500,000-1,000,000	0	0	0	0	0	0	0	3	0	1	0	4
> 1,000,000	1	0	4	2	0	6	7	11	9	9	1	50
Unclear	0	0	1	0	2	5	6	5	5	9	1	34
Total	1	0	5	2	6	15	21	30	36	36	7	159

Table 7: Distribution of Studies by Data Availability.

Data Availability	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
Yes	0	0	0	0	1	5	3	2	7	8	3	29
Yes (ext)	0	0	1	1	0	1	3	8	12	10	0	36
Upon request	0	0	0	0	0	0	0	0	1	2	3	6
Partially	0	0	0	0	0	0	0	0	0	1	0	1
No	1	0	4	1	5	9	15	20	16	15	1	87
Total	1	0	5	2	6	15	21	30	36	36	7	159

5.4 Machine Learning and Distribution

The studies applied different types of analysis to the blockchain data:

- **Classification**. The paper addressed the application of a supervised learning approach and attempted to predict a label.
- **Clustering**. The paper addressed the application of an unsupervised learning approach and attempted to group data points together.
- **Deep Learning**. The paper addressed the application of a neural network with multiple layers.
- **Regression**. The paper addressed the application of a supervised learning approach and attempted to predict a continuous value.
- **Time Series Analysis**. The paper aimed to analyze a time series.
- **Combination**. The paper addressed the application of at least two algorithms belonging to the aforementioned categories.

Table 8 shows a summary of the distribution of the selected studies by machine learning type.

Table 8: Distribution of Studies by Model.

Model	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	Total
Classification	0	0	1	0	3	7	11	14	24	13	1	74
Clustering	1	0	1	1	2	2	1	2	1	2	1	14
Deep Learning	0	0	0	0	0	0	2	5	3	2	0	12
Regression	0	0	0	0	0	3	0	1	1	3	0	8
Time Series Analysis	0	0	3	0	1	0	2	0	0	1	0	7
Combination	0	0	0	1	0	3	3	8	7	14	4	40
Other	0	0	0	0	0	0	2	0	0	1	1	4
Total	1	0	5	2	6	15	21	30	36	36	7	159

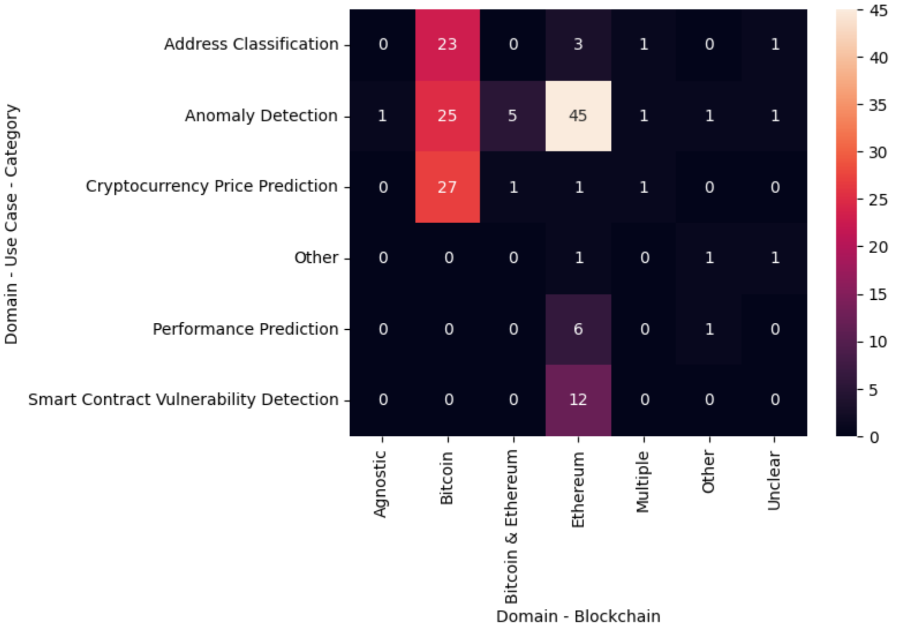

Figure 2: Distribution papers by Use Case and by Blockchain

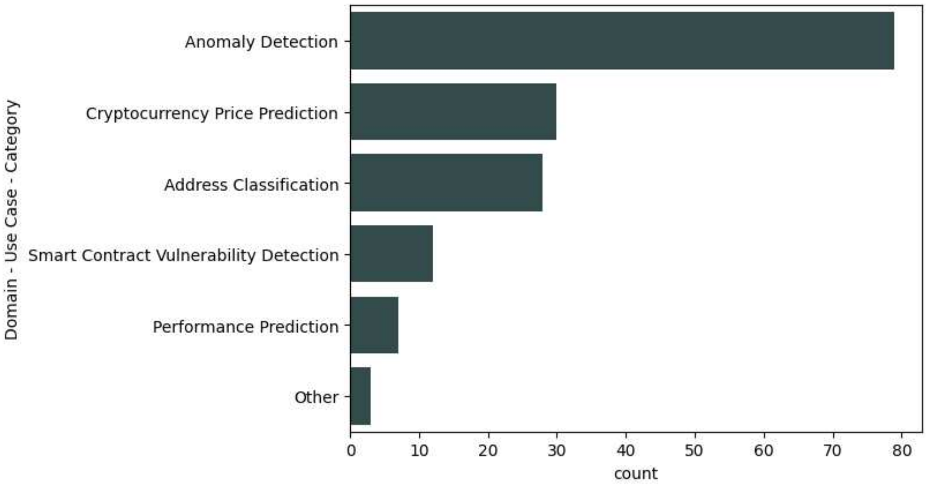

Figure 3: Distribution of papers by Use Case

6 Mapping Results

As mentioned before, the goals of this study are to provide an overview of the state of the art and to identify potential research gaps. We used heatmaps here that allow us to quickly grasp the dimensions explored by current research. The mapping results are represented in Figures 2 to 10.

The first dimension of our classification scheme, namely the Use Case, is discussed in more detail in Sections 6.1 to 6.6. The studies will be discussed by use case and we will address the other dimensions of our classification scheme as well, specifically the blockchain, the data, and the machine learning model. We can already state that, as shown in Figure 3, the majority of the studies we considered here addressed the problems of "Anomaly Detection" (49.7%), "Cryptocurrency Price Prediction" (18.9%), and "Address Classification" (17.6%). A smaller number of studies focused on "Smart Contract Vulnerability Detection" (7.5%) or "Performance Prediction" (4.4%). Three studies (1.9%) were classified as "Other". [49] proposed a method for behavior pattern clustering for blockchain nodes; [50] designed a solution to automatically label unknown contracts on Ethereum; and finally [51] conducted some data analysis on EOS blockchain data.

As far as the blockchains are concerned, we can see from Figure 4 that the majority of studies focused on a single particular blockchain, either Bitcoin (47.1%) or Ethereum (42.8%). Some authors worked on both (3.8%) or on other multiple blockchains (1.9%), e.g. Bitcoin, Ethereum and Ripple as in [52] or EOSIO and Ethereum [53]. Finally, some studies analyzed the EOSIO blockchain [51], Hyperledger Fabric [54], Steem [55]; or it was

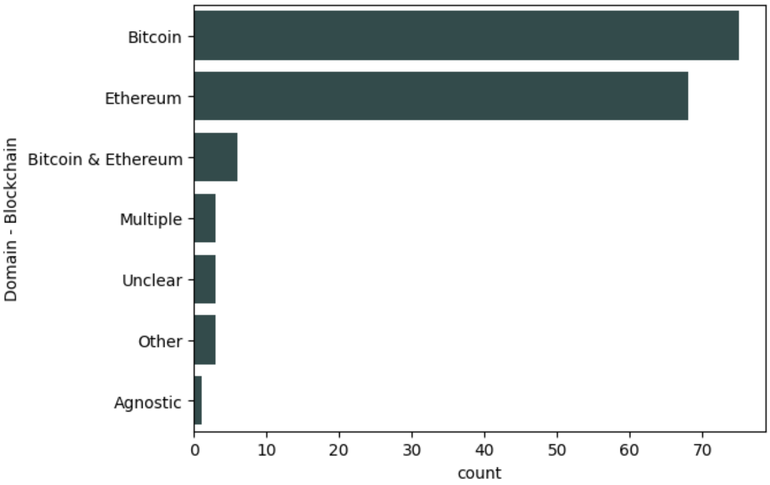

Figure 4: Distribution of papers by Blockchain

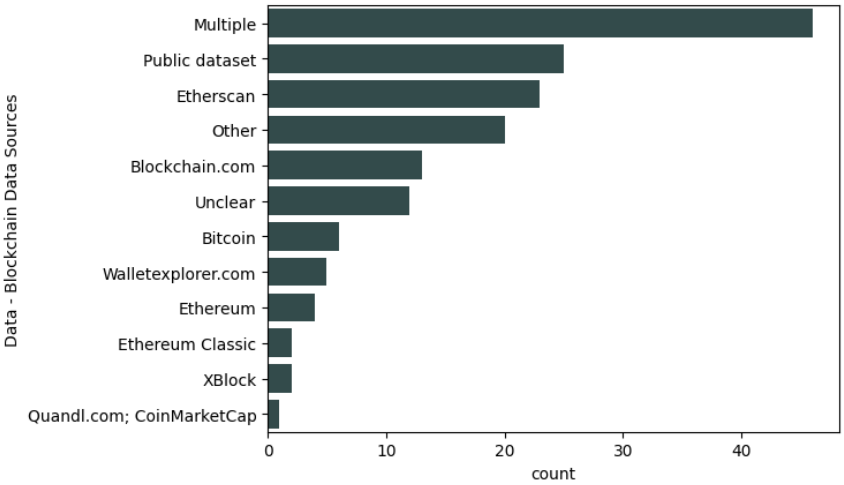

Figure 5: Blockchain Data Sources

unclear which blockchain(s) was (were) analyzed.

Next, Figure 5 shows that the majority of the studies analyzed here used multiple data sources (29.6%), such as Blockchain.com, Etherscan.io, a public dataset, and/or bitcoin clients. Other common sources include a single blockchain explorer website (27.0%) such as Blockchain.com, Etherscan.io, Walletexplorer.com, or XBlock.pro; or a public dataset (17.0%).

We can also see from Figure 6 that most studies had a dataset consisting of more than 1,000,000 data points (31.4%), between 100,000 and 500,000 data points (12.6%), or between 10,000 and 50,000 data points (10.1%). We should also note that a part of the studies we analyzed here (21.4%) were unclear regarding the size of the dataset.

Furthermore, Figure 7 displays the research data availability. Most studies did not share the data they used for the research (54.7%), some were made available by the authors (18.2%), and some were available by default because of their public characteristic (22.6%). A small number of studies stated that the data were available on request (3.8%), while the data for one study (0.6%) were partially available.

Additionally, Figure 8 shows that the period covered by the datasets fall mostly between 2013 and 2019.

Finally, when we look at the models applied to the data, we can see in Figure 9 that a large majority of the studies conducted a classification (46.5%). The second most popular processing was a combination of models (25.2%), such as classification and clustering, classification and deep learning, or classification and regression for instance. Other frequent models include clustering alone (8.8%) and regression alone (5.0%). Some authors used time series analysis (4.4%) or deep learning (7.5%).

As far as the specific algorithms are concerned, we can state from Figure 10 that the Random Forest and the Support Vector Machine were the most popular ones in the studies we cover here, followed by the Logistic Regression, XGBoost, and K-Nearest Neighbors.

In the next subsections, we discuss each use case in more detail. For each use case, we provide a summary

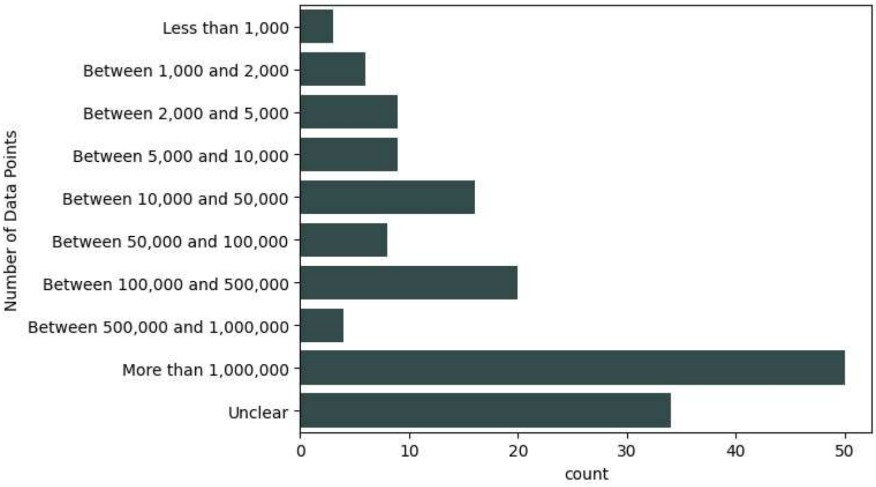

Figure 6: Blockchain Data Points Analyzed by Different Studies

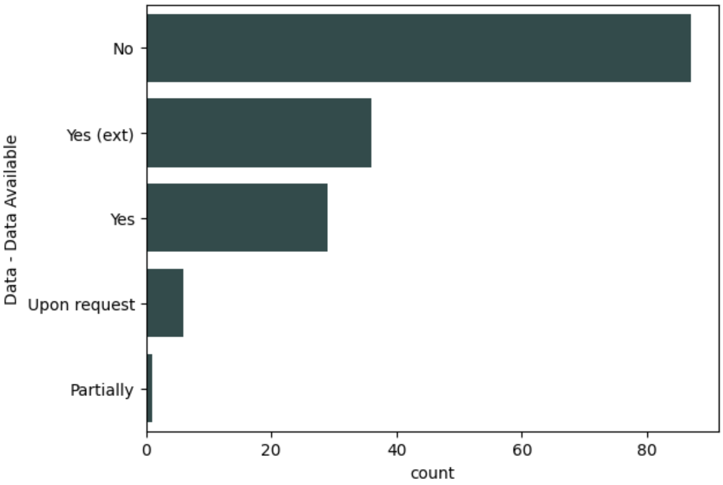

Figure 7: Distribution papers by Data Available

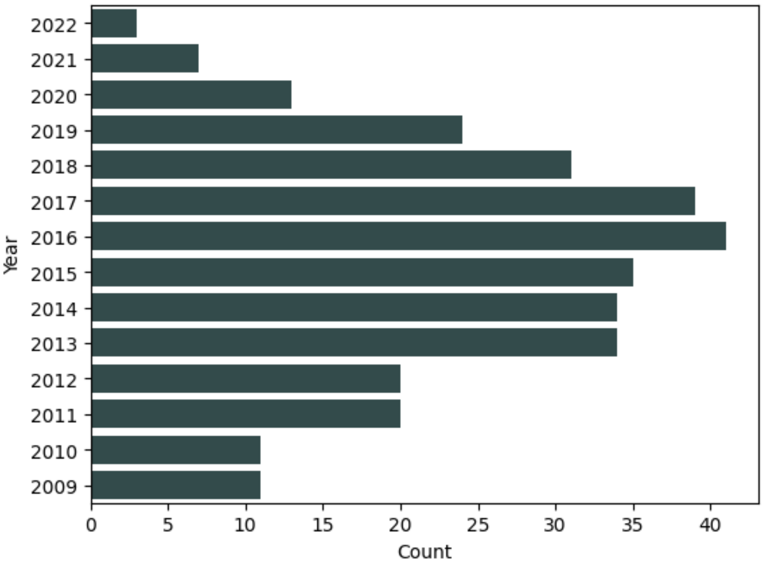

Figure 8: Distribution of papers by Period Covered

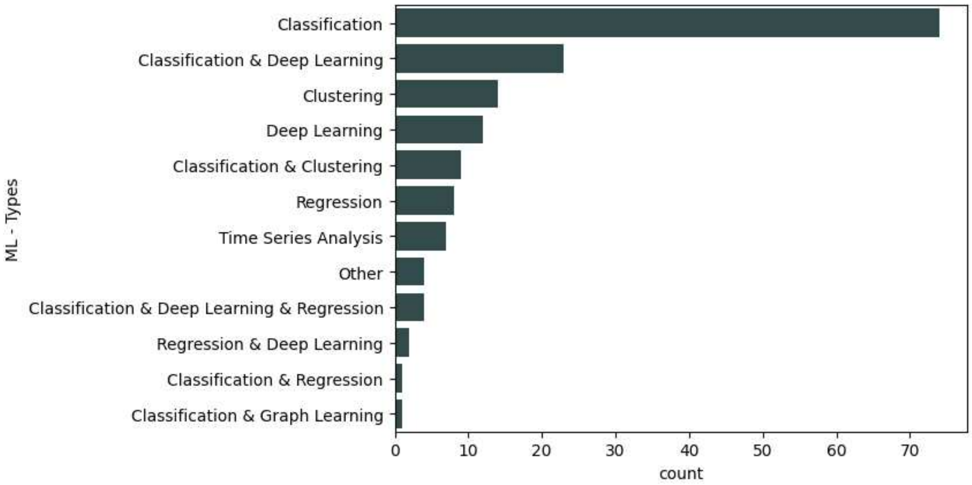

Figure 9: Distribution of papers by Type of Machine Learning Task

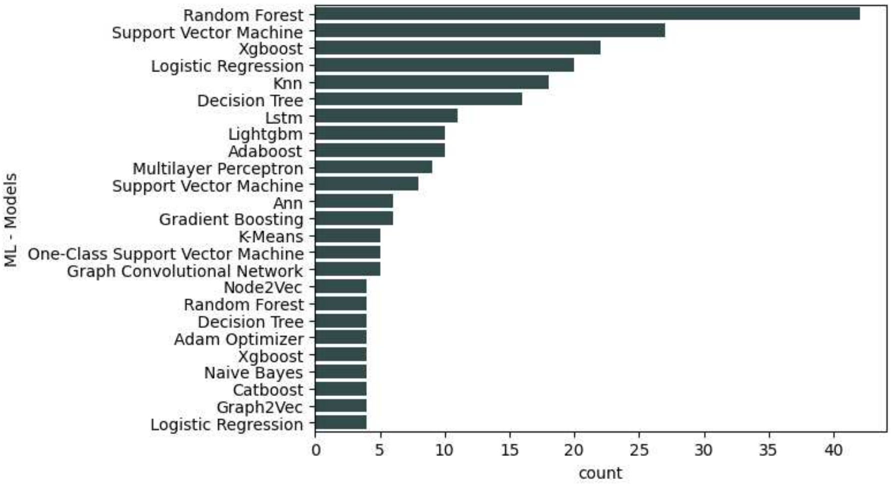

Figure 10: Distribution papers by Machine Learning Methods

table reporting: the blockchain studied, the availability of the data and code (Data-Code), and the models and the performance measures used by the authors. We provide the best performance reported by the authors (in parenthesis) and the algorithms used to achieve that performance (in bold). Note that when no performance appears in the table, it means that either it was not explicitly mentioned, or that it was graphically represented in the paper. Also, when multiple ML models are highlighted, it means that some performed best on some metrics, while other algorithms performed best on some other measure. Finally, when experiments were carried out on various datasets, or when the performance measures were reported for the train and test sets; we decided to report only the best measure. When experiments were carried out on various blockchains, we provided the metrics for both platforms.

6.1 Address Classification - De-Anonymization

We found twenty-eight papers studying address classification.

In our study, fourteen papers addressed de-anonymization or actors identification. Out of this set, fourteen papers focused on Bitcoin. Multiple authors applied a classification task using different algorithms: NB [56]; AdaBoost, Linear SVM, LR, Perceptron, RF [57]; Multivariate Wald-Wolfowitz test [58]; AdaBoost, Bagging, DT, Extremely Randomized Trees, GB, NN, RF [59]; AdaBoost, Bagging, DT, Extra Trees, GB, KNN, RF [60]. Various sets of features were fed to these algorithms: transaction-related features [56, 58, 59, 60]; transaction-related features and graph-related features [57]. The datasets used in these studies consisted of more than 1,000,000 data points [56, 58, 59, 60], and covered different periods: from September 29, 2011 to April 22, 2015 [57]; and until April 7, 2013 [58].

Various authors addressed the problem of Bitcoin de-anonymization using a clustering algorithm and transaction-related features [61, 62, 63] . In [64, 65], the authors improved the Louvain clustering algorithm in order to make Bitcoin de-anonymization possible, using a significant amount of Bitcoin transactions (almost 300 millions, and more than 120GB respectively) and two sets of features: transaction-related features and tracing data features. The other datasets consisted of more than 1,000,000 data points[61, 62], covering a period of about two months (March 10, 2020 to May 09, 2020) for [61].

Finally, four papers applied both Classification and Clustering: CatBoost, DT, XGboost [66]; KNN [67]; and RF and various clustering models (Contraction, SharedUser, K-Clique) [68]. The datasets consisted of 23 features describing output transaction links [66]; of address statistical features and address transaction history features [67]; or on-chain data and off-chain data [68]. Their size varied, from more than 1,000,000 data points [68], to less than 1,000,000 data points [66], and less than 500,000 [67]; and covered large periods of time: January 3, 2009 to January 25, 2021 [66]; and from January 2009 to September 2016 [67]. Also, [69] proposed an Adaptive Weighted Attribute Propagation (AWAP) enhanced community detection model. For their solution, the authors selected 16 transaction-related features, and used a dataset consisting of less than 10,000 data points.

[53] focused on identity inference on EOSIO and Ethereum, using a dataset consisting of less than 5,000 accounts. The authors applied GNN to subgraphs centered on target accounts.

In our study, eleven papers focused on address classification. The majority (seven papers) of them studied address classification on Bitcoin, using: ANN and RF [70]; Adaboost, DT, and imECOC [71]; AdaBoost with DT, LightGBM, LR, MLP, NN, RF, SVM, XGBoost [72]; RF [73]; AdaBoost, GB, RF [74]; ABC, BG, CART, ET, GB, KNN, LDA, LR, MLP, NB, RFC, SGD, SVM [75]; and C4.5, ID3, KNN, PART [76]. As far as the selected features are concerned, [70] used transaction-related features, making the distinction between transmission and recipient addresses; [71] used address-related features and network metrics; [72] used three types of features, namely basic statistics, extra statistics, and moments; [73, 75, 76] extracted transaction history features; [74] used four sets of features, specifically entity features, address features, and two graph-related features. The periods covered by the datasets in the studies here: from January 1, 2016 [70]; from January 3rd, 2009 to June 30, 2018 [72]; from January 9, 2009 to February 9, 2017 [73]; from the Bitcoin genesis until February 2019 [74]; and the period 2011-2018 [76]. These periods led to a dataset size of: less than 1,000,000 data points [70]; of more than 1,000,000 data points [72, 74, 76, 71]; of less than 500,000 data points [73]; less than 100,000 data points [75]

One paper applied classification and deep learning to study the address classification, clustering and coin mixing problems on Bitcoin. Specifically, the authors in [77] trained the following algorithms: LINE, LSTM Transaction Tree, RF using GCN Feature, SGD optimizer. The authors used sequence features extracted from transaction trees; and used a dataset of more than 1,000,000 data , covering the following periods: (i) November 16, 2013 to May 10, 2014; (ii) May 12, 2016 to May 17, 2016.

Only two papers studied address classification on Ethereum. [78] focused on address clustering and de-anonymization, using a dataset of more than 1,000,000 data points, spanning from July 30, 2015 to April 4, 2020. The authors applied Node Embeddings. In [79], the authors, using a dataset of more than 1,000,000 data points, applied a classification task and a deep learning task. They selected node features; and fed them to the following algorithms: Adam Optimizer, Cluster-GCN, Filter and Augment Graph Neural Network, GCN, GNN, GraphSAGE, H2GCN.

Finally, [80] proposed PeerClassifier, a solution for blockchain peers classification, using the daily transaction amounts of peers extracted as a sequence.

Other papers (two in our study) centered on agent characterization. [81] studied entities characterization on Bitcoin. The authors collected more than 1,000,000 data points, using blocks created before March 24 2018. The dataset was composed of five feature classes (address features, entity features, temporal features, centrality features, and motif features), and was fed to LightGBM and LR. [82] focused on characterizing key agents on Ethereum. The authors collected data between May 2, 2016 to June 29, 2019, for a total of less than 50,000 data points. They selected 28 features (categorized as volume features, temporal features, and structural features) and fed them to multiple classifiers (LightGBM, LR, MLP, RF, SVM).

Paper	Blockchain	Data-Code	Model	Performance
[66]	Bitcoin	N-N	Classification: Decision Tree, **CatBoost**, **XGBoost**; and Clustering	Clustering: aNMI (0.796), Completeness (0.6661), Homogeneity (1.0), Rand Index (0.532), V-score/NMI (0.796); Classification: ROC-AUC score (1.0)
[69]	Bitcoin	Y-N	Classification: **AWAP** (Enhanced Community Detection Model), BAGC, CP, DT, **LightGBM**, LR, RF, XGBoost; and Clustering: **AWAP** (Enhanced Community Detection Model), Big-CLAM, CESNA, Circles, CNM, CODICIL, CP, DeepWalk	Classification: Accuracy (0.95), F-Score (0.92), Precision (0.91); Clustering: F-Score (0.7583), Jaccard (0.5875), NMI (0.5683)
[82]	Bitcoin	Y-N	Classification: LR, SVM, MLP, **RF**, LightGBM	Accuracy (0.893), F1 (0.985), Precision (1.0), Recall (0.98), Macro F1 (0.865), Macro Precision (0.888), Macro Recall (0.862)
[53]	EOSIO and Ethereum	Y-N	Classification and Deep Learning: **I^{2}BGNN** (Graph Neural Network), KNN, RF, SVM	F1 (0.9950), Precision (0.9917), Recall (0.9986)
[81]	Bitcoin	N-N	Classification: **LightGBM**, LR	Accuracy (0.92), F1 (0.91), Precision (0.92)
[56]	Bitcoin	Y-N	Classification: NB	Unclear
[61]	Bitcoin	N-N	Clustering: “Multi-Input Addresses” heuristic	Reliability
[70]	Bitcoin	N-N	Classification: ANN, **RF**	Accuracy (0.844)
[71]	Bitcoin	N-N	Classification: Adaboost, DT-CART, **DT-HDDT**), **imECOC**	Accuracy (0.9147), AUC (0.9051), F1-measure (0.9117), G-mean (0.8283)
[63]	Bitcoin	N-N	Clustering	Unclear

[57]	Bitcoin	N-N	Classification: AdaBoost, Linear SVM, LR, Perceptron, **RF**	F1 (0.9973), Precision (0.9971), Recall (0.9976)
[62]	Bitcoin	Y-N	Clustering	aNMI (0.67), F1 (0.86), NMI (0.89), Precision (0.98), Recall (0.91)
[67]	Unclear	N-N	Classification: KNN; and Clustering	Accuracy (0.911), F1 (0.787), False Accept Rate (0.051), Precision (0.813), Recall (0.772), Validation rate (0,869)
[80]	Unclear	N-N	Classification: DT, KNN, **PeerClassifier**, SVM	Accuracy (0.745)
[68]	Bitcoin	N-N	Classification: RF; and Clustering: Baseline, Contraction, **K-Clique**, SharedUser	Classification: Accuracy (0.738), F1 (0.701), Precision (0,769), Recall (0.654); Clustering: aMI (0.2394), Rand index adjusted for chance (0.03), V-measure (0.5229)
[64]	Bitcoin	N-N	Clustering	Accuracy (1.0), Comprehensiveness (1.0)
[65]	Bitcoin	N-N	Clustering	Accuracy (0.91), Recall (1.0)
[58]	Bitcoin	Y-N	Classification: Multivariate Wald-Wolfowitz test	Accuracy (0.563), Equal Error Rate (0.084)
[59]	Bitcoin	N-N	Classification: Adaptive Boosting, Bagging (Bootstrap Aggregation), DT, Extremely RT, **GB**, k-NN, RF	Accuracy (0.8042), F1 (0.7964), Precision (0.8055), Recall (0.8083), ROC Curve
[60]	Bitcoin	N-N	Classification: AdaBoost, Bagging Classifier, DT, Extra Trees, **GB**, KNN, RF	Accuracy (0.78), F1 (0.76), Precision (0.75), Recall (0.78), Support (451)
[78]	Ethereum	Y-Y	Classification: Node Embeddings	AUC, Average rank
[72]	Bitcoin	Y-N	Classification: AdaBoost, **LightGBM**, LR, **NN**, Perceptron, RF, SVM, XGBoost	Macro-F1 (0.86), Micro-F1 (0.91)
[73]	Bitcoin	Y-N	Classification: RF	Accuracy (0.72)
[74]	Bitcoin	N-N	Classification: Adaboost, **GB**, **RF**	Accuracy (0.9968), F1 (1.0), Matthews Correlation Coefficient (0.99), Precision (1.0), Recall (1.0), Standard Deviations

[77]	Bitcoin	Y-Partially	Classification: Large-scale information network embedding , RF; and Deep Learning: **LSTM Transaction Tree**, **RF using GCN Feature**, SGD Optimizer	Classification: Accuracy, F1(0.983), Precision (0.982), Recall (0.990)
[79]	Ethereum	N-N	Classification and Deep Learning: Adam Optimizer, Cluster-GCN, **Filter and Augment GNN**, GCN, GraphSAGE, H2GCN	Macro-F1 (0.866), Macro-Precision (0.876), Macro-Recall (0.871), Micro-F1 (0.888)
[75]	Bitcoin	N-N	Classification: AB, BG, CART, ET, **GB**, KNN, LDA, LR, MLP, NB, RF, SGD, SVM	Accuracy (0.8076), F1 (0.8056), Precision (0.8027), Recall (0.8271), Support (214)
[76]	Bitcoin	Y-N	Classification: C4.5, ID3 algorithm, KNN, PARTial Decision Tree (PART)	Accuracy, Kappa (Cohen's Kappa)

Table 9: Papers Addressing Address Classification

6.2 Anomaly Detection

In our study, we analyzed seventy-nine papers addressing Anomaly Detection: Ponzi Scheme Detection (10 papers), Phishing detection (12 papers), Ponzi Scheme and Phishing detection (1 paper), Intrusion or Attack Detection (4 papers), Illicit account detection (23 papers), Misbehavior or fraud detection (27 papers), and Bot detection (2 papers).

In our study, we found ten papers working specifically on **Ponzi scheme detection**. All approaches focus on Ethereum, except for [83] who address the problem on Bitcoin. The authors built and made publicly available a dataset consisting of about 10,000 addresses and features of Bitcoin Ponzi schemes. As far as the papers focusing on Ethereum are concerned, authors used key account features and opcodes [84, 85, 86, 87], transaction features and code features [88], only the opcodes [89, 90, 91], transaction features, features and bytecode [87]. The authors exploited a dataset consisting of: 1250 non-Ponzi scheme contracts and 131 Ponzi scheme contracts [84, 92], 200 Ponzi scheme contracts and 3580 non-Ponzi scheme contracts [85, 89, 91], 3203 non-Ponzi scheme contracts and 172 Ponzi scheme contracts [88], 168 Ponzi schemes and 2851 normal smart contracts (the XBlock dataset) [86], 386 Ponzi schemes and 3239 non-Ponzi schemes [90], 3614 Non-Ponzi contracts and 810 Ponzi contracts [91] The classifiers applied were: XGBoost[84, 89, 85], RF [89, 91, 88], SGD and J48 [88], DT [89, 85, 91], Extremely Randomized Trees [89, 91], GB [89, 91], LightGBM [89, 87], Logistic Regression [89], SVM [89, 85], Behavior Forest [92], Oversampling-based LSTM [86], Ordered Boosting [90], AdaBoost, combination of Bagging-Tree and XGBoost, KNN [91], Isolation Forest [85].

Multiple authors addressed **phishing detection** on Ethereum, using classification and/or deep learning. They used different types of models: CT-GCN, Line graph and GCN, LR, One-Class SVM, SV, and XGBoost [93]; LightGBM, DeepWalk, Node2Vec, LINE, GCN [94]; SVM [95]; Graph2Vec, Line Graph2Vec, Node2Vec, and WL-kernel [96]; IF, LR, NV, One-Class SVM [97]; Graph2Vec, Node2Vec, Sub2Vec [98]; AdaBoost, KNN, SVM [99]; Adam optimizer, BPNN, DT, LightGBM, LR; LSTM, LSTM-FCN, Node2Vec, RF, RNN, SVM, Trans2Vec; [100]; GATNE-I (network embeddings), GNN, Random Walk[101]; DeepWalk, EGAT, GAT, GCN, Graph2Vec, GraphSageNode2Vec, MLP, Softmax (comparison with previous works where DElightGBM, LightGBM, MP-GCN, RF were used), Sub2Vec [102]; Adam optimizer, GCN, GIN, Graph2Vec, GraphSAGE, SF [103]; 48 Consolidated, C4.5 DT, Eth-PSD, Fast Decision Tree, JRip, NB Tree, OneR, PART Decision List [104]. The inputs for these models were graph-based (transactional) features [93, 94, 96, 98, 101, 102, 103, 97], account features and network features [99], transaction features, state features, and transfer features [100], and transaction-based features [104, 95]. The datasets were composed of reconized phishing accounts and recognized non-phishing accounts; and were balanced [93, 96, 102] or unbalanced [94, 98, 99, 100, 104].

[105] addressed both Ponzi schemes and phishing scams detection on Ethereum using data mining techniques. To address the first type of misbehavior, the authors extracted seven account features and used the opcodes of the smart contracts. They fed these features to an XGBoost algorithm and used a dataset consisting of 10,000 transactions. As far as the phishing scam detection problem is concerned, the authors used 7,795,044 transactions and compared multiple classifiers (DT, Dual-sampling Ensemble SVM, Dual-sampling Ensemble DT, Dual-sampling Ensemble lightGBM, LightGBM, and SVM).

Multiple papers in our study addressed **fraud detection** on Bitcoin [106, 107, 108, 109, 110, 111], on Ethereum [112], and on Bitcoin and Ethereum [113, 114, 115]. Various algorithms were used: an improved apriori algorithm [106]; k-means and a trimmed k-means [107]; Boosted LR, kd-trees, maximum-likelihood based LR, RF, Trimmed k-means [108]; RF and XGBoost [109], LR, RF, XGBoost, and Angle-based Outlier Detection, Cluster-based Outlier Factor, Isolation Forest, KNN, Local Outlier Factor, One-Class SVM, and PCA [110]; k-means [111]; AB, BT, DT, Ensemble models, ET, GB, LGBM, RF, XGB [112]; RF, XGBoost [113] ; Adam optimizer, GCN, MLP decoder [114]; and LR, RF, SVM [115]. The Elliptic dataset [116] was used by [110] and used and augmented by [114]. The sets of features selected or extracted by the authors include: transaction features [106, 109, 110, 113]; currency features, network features, and average neighborhood features [107, 108]; Turnover-features, connectivity-features, activity-features, utxos-specific-features [111]; opcode n-grams, transaction data, source code characters [112]. Except for [110, 113, 109], the dataset consisted of more than 1,000,000 data points.

Next, 17 papers addressed **abnormality detection** on Bitcoin [117, 118], on Ethereum [119, 120, 121, 122, 123, 124, 125, 126, 127], and on Bitcoin and Ethereum [128, 129, 130, 131, 132, 133]. The authors addressed the problem using classification, deep learning and/or clustering: ANN and RF [117]; GCN [118]; Extra Trees, GB, LR, MLP, RF, and XGBoost [128]; AdaBoost, CatBoost, DT, KNN, LightGBM, LR, MLP, RF, SVC, and XGBoost [129]; AdaBoost, KNN, LOF, Mahalanobis distance-based method, MLP, OCSVM, RF, and SVM [130]; KNN, NB, and SVM [131]; BTCOut, CTOuliers, DBSCAN, k-medoids algorithm, OddBall, Tclust [132]; Apriori, Self Organised Maps [119]; k-means and RF [127]; GCN, GNN, IForest, OC-GAT, OC-GCN, OC-SAGE, OCSVM [120, 121]; DT, Kernel SVM, KNN, LR, NB, RF, and One-class SVM [122]; CNN, GAT, GCN, Heterogeneous Graph Transformer Networks, RCNN, SVM [123]; sequence to sequence recurrent autoencoder [124]; LSTM [125]; DT, Isolation Forest and RF [126]; and K-Means [134]. The Elliptic dataset [116] was used by [118, 128, 129] and was augmented for the authors studying Ethereum in addition to Bitcoin. The Ethereum Classic dataset [135] (composed of 2179 fraudulent accounts and 2502 normal accounts) was used in [122, 124]. The size of the datasets used in these studies varied from more than 1,000,000 data points [117, 130, 132, 133, 119, 121, 124], and less than 500,000 data points [131, 127, 120, 122, 123, 125, 126]. The features used as input for the models include: transaction-based features [117, 131, 122, 125, 126]; graph-based transaction features or transactions depicted as graph [130, 132, 133, 120, 121]; addresses (Smart Contract addresses and user addresses) and transactions [119]; features extracted from wallet transaction and wallets data [127]; account and code features [123]; blocks features and transaction features [124]; and time series transaction data [134].

In our study, 23 papers addressed the **illicit account or illicit node detection** problem on Bitcoin [136, 137, 138, 139, 140, 141, 142, 143, 144, 145] and on Ethereum [146, 135, 147, 148, 116, 149, 150, 151, 152, 153, 154, 155, 156]. For this class of problem, various algorithms were used: DT, IF, IS, LR, OCSVM, PU learning [136]; ANN, LSTM, RF, SVM with RBF kernel, and XBGoost [137]; GB and RF [138]; LR, RF, and SVM [139]; Evolve-GCN, GCN, GCN and MLP, LR, MLP, RF, Skip-GCN, Temporal GCN [140]; GCN, Graph Enhanced RF with Feedback model, Graphlet Spectral Correlation Analysis, RF; and Regression [141]; AdaBoost, BN, k-means, NB, and RF [142]; CatBoost, LGBA, RF, XGBoost [143]; GCN, Node Embeddings, MLP [144]; Attention Mechanism-based GCN, GCN, MLP, MP-GAT, Node Embeddings, Skip-GCN [145]; RF, SVM, and XGBoost [146]; XGBoost [135]; Birch algorithm [147]; ASXGB, CatBoost, LGB, RF, XGBoost [148]; DT, GB, KNN, MLP, RF, SVM [149]; ETH Tracking Tree Method, LightGBM, LSTM; RF, XGBoost [150]; Ensemble methods, LR, RF, and SVM [151]; DT (J48), KNN, and RF [152]; AdaBoost, KNN, LGBM, LR, MLP, RF, SVM, and XGBoost [153]; C5, CatBoost, CAT Tree, LGB, NN, SVM; and Clustering [154]; LR, SVM, and XGBoost [155]. Multiple authors used the Elliptic dataset to train and test their models [139, 140, 141, 142, 143, 144, 145, 148] or the Ethereum Classic dataset [143, 153, 154], or another public dataset [157] consisting of 10 millions of transactions [147]; otherwise, the authors collected their own data: [136] collected 3 snapshots of 1,500,000 Bitcoin transactions; [137] used 24,720 illicit addresses and 1,209,850 licit addresses; [138] exploited 21 Darknet Market-related and 351 non-Darknet Market-related Bitcoin entities with the corresponding addresses and transactions; [146] collected 2,200 wallets documented as involved in illegal activity and transactions from 349,999 randomly selected non-fraudulent wallets; [149] collected blocks between 9,000,000 and 10,999,999, and 16,108,509 addresses and 141,242,377 transactions; [150] used 5585 labeled addresses; [151] took advantage of 18,000,000 transactions; [152] used 7,809 transactions (7,651 normal and 159 fraudulent transactions); and [155] used 2,600 illicit labeled addresses and 20,000 random addresses. As far as the features are concerned, the authors extracted and used: topological and temporal features [137]; transaction-based, address-based, block-based and statistics [138]; local features, local and aggregated features, local and node embeddings, and aggregated and node embeddings [139, 148]; local features [140]; local and aggregated features [144]; normal transaction-based features and erc20 token transaction-based features [135]; Ether trading transactions, smart contract creation and smart contract invocation and account-based features (external owned account and smart contract account) [147]; local and global features [149]; transaction-based features and sequence features (information of the ETH flow) [150]; general features, neighborhood features, local features, timestamp-related features [151]; transaction-based features [152, 146]; account data, transactional data, and history data [155]. Finally, [156] proposed SigTran, a graph-based method for the detection of illicit nodes on Ethereum and Bitcoin. The authors used the dataset made public by [116] and extracted four sets of features: structural features, transactional features, regional features, and neighborhood features. They reported a better performance for their tool, compared to existing works. Specifically, the results for the Bitcoin and Ethereum blockchains respectively were: precision scores were 0.905 and 0.944, the recall scores were 0.947 and 0.940, the F1 scores were 0.918 and 0.942, the accuracy scores were 0.915 and 0.942, and the AUC scores were 0.976 and 0.976.

Four papers in our study focus on **attack or intrusion detection** on Ethereum [158, 159] and on Bitcoin, Bytecoin and Monero [160], using Classification and/or Deep Learning: LSTM and RNN [158]; CNN, DT, KNN, and MLP [159], RF [160]; and DT, Ensemble methods, KNN, MLP, SGD, and SVM [161]. The datasets in these studies consisted of block-related features, gas-related features, and transaction-based features (Ethereum Classic dataset) [158]; of transaction-based features, block-based features, blockchain-based features [159]; and of traffic-related features [160].

Finally, a couple of papers worked on **bot detection**. [162] proposed a solution for bot detection on the Bitcoin blockchain, using a One-class SVM . With a dataset consisting of more than 100,000 data points, and consisting of about 15 transaction-related features. [55], on the other hand, worked on the same problem but focused on the Steem blockchain, and more specifically on posting bot detection on the Steem blockchain. The authors collected data about 984 accounts, divided into 325 bot accounts and 659 human accounts. They extracted various post-related features using the Minimum Average Cluster from Clustering Distance between Frequent words and Articles. Finally, they tested various classifiers (AdaBoost, DT, LightGBM, LSV, MLP, RF with Entropy, RF with Gini, XGBoost).

Paper	Blockchain	Data-Code	Model	Performance
[158]	Ethereum	N-N	Deep Learning: LSTM, RNN	Confusion matrix
[131]	Bitcoin	N-N	Classification: KNN, NB, **SVM**	Energy value, Accuracy (0.98)
[123]	Ethereum	Y-N	Classification and Deep Learning: CNN, GAT, GCN, **Heterogeneous Graph Transformer Networks**, RCNN, SVM	Macro-F1 (0.82), Micro-F1 (0.83)
[86]	Ethereum	Y-N	Classification: Recurrent Neural Network - LSTM	F (0.96), Precision (0.97), Recall (0.96)
[128]	Bitcoin and Ethereum	Y-N	Classification: Extra Trees, GB, LR, MLP, **RF**, **XGBoost**	Accuracy (0.9802 - 0.9891), AUC (0.951 - 1.0), F1 (0.8239 - 0.9760)
[160]	Bitcoin, Bytecoin, Monero	N-N	Classification: **RF**	AUC (0.9908), F1 (0.96), FPR, TPR
[90]	Ethereum	N-N	Classification: **Ordered Boosting**	F (0.96), Precision (0.95), Recall (0.96)
[135]	Ethereum	N-N	Classification: **XGBoost**	Accuracy (0.963), AUC (0.994)
[91]	Ethereum	N-N	Classification: AdaBoost, **combination of Bagging-Tree and XGBoost**, DT, Extra trees, GB, KNN, RF	Accuracy, AUC, F1 (0.95), FNR, FPR, Precision (0.97), Sensitivity (0.93), TNR, TPR
[161]	Unclear	N-N	Classification: Ensemble methods, DT, KNN, MLP, SGD, SVM	Accuracy, Precision, Recall

[105]	Ethereum	Y-N	Classification: DT, Dual-sampling Ensemble DT, Dual-sampling Ensemble, **Dual-sampling Ensemble lightGBM**, LightGBM, SVM, XGBoost	AUC (- - 0.8097), F (0.86 - -), F1 (- - 0.8122), Precision (0.94 - 0.8196), Recall (0.81 - 0.8050)
[134]	Agnostic	N-N	Clustering: **K-Means**	Accuracy (0.982)
[93]	Ethereum	Y-Y	Classification and Deep Learning: **CT-GCN**, Line graph and GCN, LR, One-Class SVM, SV, and XGBoost	Accuracy (0.8808), F1 (0.8814)
[118]	Bitcoin	Y-N	Deep Learning: ARMAConv, **ClusterGCNConv**, GAT, GCN, GNN-FiLM, GraphConv, GraphSAGE, LEConv, Linear Regression, LR, MFConv, MLP, SGConv, SuperGATConv, **TAGCN**, TransformerConv	F1 (0.7298), Precision (0.9527), Recall (0.6334)
[146]	Ethereum	N-N	Classification: **RF**, **SVM**, **XGBoost**	F1 (0.4470), FN, FP, FPR (0.002), Precision (0.8571), Recall (0.8747), Specificity (0.9998), TN, TP
[121]	Ethereum	Y-N	Deep Learning: IForest, **OC-GAT**, OC-GCN, **OC-SAGE**, OCSVM	Accuracy (0.9075), AUROC, F1 (0.8346)
[156]	Bitcoin and Ethereum	Y-Y	Classification: Node2Vec, RiWalk, **SIGTRAN (LR)**	Accuracy (0.915 - 0.942), AUC (0.976 - 0.976), F1 (0.918 - 0.942), Precision (0.905 - 0.944), Recall (0.947 - 0.940)
[124]	Ethereum	Y-N	Deep Learning: Sequence to sequence recurrent autoencoder	Unclear
[84]	Ethereum	Y-N	Classification: **XGBoost**	Precision (0.94), Recall (0.81), F-score (0.86)
[106]	Bitcoin	Y-N	Frequent Set Mining: A Priori	-
[94]	Ethereum	N-N	Classification and Deep Learning: DeepWalk, **GCN**, LightGBM, LINE, Node2Vec	AUC (0.5866), F1 (0.2636)), Precision (7294), Recall (0.1735))
[125]	Ethereum	N-N	Deep Learning: **LSTM**	F1 (0.77), Precision (0.88), Recall (0.70)
[137]	Bitcoin	N-N	Classification and Deep Learning: ANN, LSTM, **RF**, SVM with RBF kernel, **XGBoost**	F1 (0.9069), Precision (0.9567), Recall (0.8805)
[89]	Ethereum	Y-N	Classification: DT, **Extremely Randomized Trees**, GB, LightGBM, LR, RF, SVM, XGBoost	F1 (0.95), Precision (0.98), Recall (of 0.93)
[126]	Ethereum	N-N	Outlier Detection: DT, Isolation Forest, RF	-
[147]	Ethereum	Y-N	Clustering: Birch algorithm	-

[136]	Bitcoin	N-N	Classification: DT, IF, **IS**, LR, OCSVM, **PU learning**	FPR (0.0334), G-Mean (0.9479), TPR (0.9388)
[96]	Ethereum	N-N	Classification: Node2Vec, Graph2Vec, **Line Graph2Vec**, WL-kernel	F1 (0.73), Precision (0.69), Recall (0.77)
[162]	Bitcoin	N-N	Classification: One-class SVM	AUC (0.99), FPR (0.01), TPR (1.0)
[132]	Bitcoin	Y-N	Classification: **BTCOut**, CTOuliers, DBSCAN, k-medoids algorithm, OddBall, Tclust	F2 (0.473), Precision (0.433), Recall (0.602)
[133]	Bitcoin	N-N	Clustering: Graph-based method	-
[117]	Bitcoin	N-N	Classification: ANN, **RF**	F1 (0.9868)
[138]	Bitcoin	N-N	Classification: GB, RF	F1, Precision, Recall
[107]	Bitcoin	Y-N	Clustering: k-means, Trimmed k-means	Number known anomalies that were detected successfully
[119]	Ethereum	Partially-Y	Clustering: Apriori, Self Organised Maps	-
[151]	Ethereum	N-N	Classification: **AdaBoost**, LR, **RF**, **Stacking**, SVM	Accuracy (0.998), F1 (0.998), Precision (0.997), Recall (1.0)
[152]	Ethereum	Y-N	Classification: DT (j48), **KNN**, RF	Accuracy (0.9877), F (0.987), Precision (0.986), Recall (0.988)
[113]	Bitcoin and Ethereum	Y-N	Classification: **RF**, XGboost	AUC (0.92), Precision, Recall
[95]	Ethereum	N-N	Classification: **SVM**	F (0.846), Precision (0.871), Recall (0.822)
[97]	Ethereum	N-N	Classification: IF, LR, NV, **One-Class SVM**	F (0.908), Precision (0.927), Recall (0.893)
[85]	Ethereum	Y-N	Classification: DT, **IF**, One-class SVM, SVM, XGBoost	F (0.79), Precision (0.95), Recall (0.69)
[88]	Ethereum	Y-N	Classification: **J48**, RF, **SGD**	F (0.97), Precision (0.99), Recall (0.97)
[87]	Ethereum	Y-Partially	Classification: **Improved LightGBM**	Accuracy, AUC (0.992), F (0.967), Precision (0.967), Recall (0.967)
[92]	Ethereum	Y-N	Classification: **Behavior Forest**	F, Precision (0.956), Recall (0.93)
[143]	Bitcoin	Y-N	Classification: **CatBoost**, LGBA, **RF**, **XGBoost**	Accuracy (0.98), F1 (0.98), Recollect (0.976), Sensitivity (0.988)

[83]	Bitcoin	Y-Y	Classification: Bayes Network, **RF**, RIPPER	Accuracy (0.988), AUC (0.978), F (0.443), G-mean (0.978), Precision (0.287), Recall (0.969), Specificity (0.987)
[127]	Ethereum	N-N	Classification: **RF**; and Clustering: k-Means	F1 (0.96), Precision (0.96), Recall (0.96), Support (9632)
[109]	Bitcoin	N-N	Classification: RF, XGboost	F1, FPR, TPR
[108]	Bitcoin	N-N	Classification: **Boosted LR**, kd-trees, Maximum-likelihood based LR, **RF**; and Clustering: Trimmed k-means	Kappa (0.99), Precision (0.99), Recall (1.0), ROC (0.99), Sensitivity
[144]	Bitcoin	Y-N	Classification and Deep Learning: **GCN**, MLP, Node Embeddings	Accuracy (0.974), F1 (0.773), Precision (0.899), Recall (0.678)
[110]	Bitcoin	Y-Partially	Classification: LR, **RF**, XGBoost; and Anomaly Detection: Angle-based Outlier Detection, Cluster-based Outlier Factor, Isolation Forest, KNN, Local Outlier Factor, One-Class SVM, PCA	F1 (0.83)
[153]	Ethereum	Y-N	Classification: AdaBoost, KNN, **LGB**, LR, MLP, RF, **SVM**, XBoost; and Clustering	Accuracy (0.9860), F1 (0.9486), Precision (0.9948)
[154]	Ethereum	Y-N	Classification: C5, **CatBoost**, CAT Tree, LGB, NN, SVM; and Clustering	Accuracy (0.947), AUC (0.9846)
[145]	Bitcoin	Y-N	Classification and Deep Learning: Attention Mechanism-based GCN, GCN, MLP, **MP-GAT**, Node Embeddings, Skip-GCN	Accuracy (0.973), F1 (0.767), Precision (0.868), Recall (0.688)
[155]	Ethereum	N-N	Classification: LR, SVM, **XGBoost**	Accuracy (0.99), F1 (0.94), Precision (0.90), Recall (1.0)
[120]	Ethereum	N-N	Classification and Deep Learning: **EVANGCN**, GCN, **OCGCN**	F1 (0.8702), MicroAvg F1 (0.7788), Precision (0.7284), Recall (0.6409)
[114]	Ethereum	Y-Y	Classification and Deep Learning: Adam optimizer, **GCN**, MLP	Accuracy (0.9813), F1 (0.7735), Precision (0.8225), Recall (0.8387)
[148]	Bitcoin and Ethereum	Y-N	Classification: **ASXGB**, CatBoost, LGB, **RF**, **XGBoost**	Accuracy (0.981 - 0.989), F1 (0.940 - 0.983), Precision (0.988 - 0.985), Recall (0.931 - 0.981)

[112]	Ethereum	Y-N	Classification: AB, BT, DT, **Ensemble models**, ETC, GB, LGBM, **RF**, XGB	Accuracy (0.8967), F1 (0.8874), FNR (0.0018), FPR (0.1785), Precision (0.9837), Sensitivity (0.8148), TNR (0.9981), TPR (0.8214)
[98]	Ethereum	N-N	Classification: **Ego-Graph Embeddings**, Graph2Vec, Node2Vec, Sub2Vec	F1 (0.8199), Precision (0.8132), Recall (0.8271)
[139]	Bitcoin	Y-N	Classification: LR, **RF**, SVM	Accuracy (0.98851), Precision (0.65901), Recall (0.44866)
[99]	Ethereum	N-N	Classification: **AdaBoost**, KNN, **SVM**	Attack Success Rate, AUC (0.9276), Average number of Modified Edges, F1 (0.94), Precision (0.96), Recall (1.00)
[100]	Ethereum	N-N	Classification: DT, LR, RF, SVM; and Deep Learning: Adam optimizer, LightGBM LSTM, **LBPS** (STM-FCN and BP neural network), Node2vec, RNN, Trans2vec	Accuracy (0.9730), F1 (0.9786), Precision (0.9813), Recall (0.9759)
[140]	Bitcoin	Y-N	Classification and Deep Learning: Evolve-GCN, GCN, GCN and MLP, LR, MLP, RF, Skip-GCN, **Temporal GCN**	Accuracy (0.977), F1 (0.806), Precision (0.927), Recall (0.713)
[101]	Ethereum	N-N	Classification: DT, GATNE-I (Network Embeddings), GNN, LR, NB, **One-Class SVM**, Random Walk	F1 (0.957), PR-AUC (0.889), ROC-AUC (0.959)
[122]	Ethereum	Y-N	Classification: **DT**, Kernel SVM, KNN, LR, **NB**, One-class SVM, **RF**	Accuracy (0.99), Detection rate (0.953), FPR (0.0005)
[141]	Bitcoin	Y-N	Classification and Deep Learning: GCN, **Graph Enhanced RF with Feedback model**, Graphlet Spectral Correlation Analysis, RF; and Regression	F1 (0.821)
[111]	Bitcoin	Y-N	Clustering: k-Means	CoinJoin-related metrics
[149]	Ethereum	Y-N	Classification: DT, **GB**, KNN, MLP, **RF**	Accuracy (0.985), F1 (0.743), Precision (0.682), Recall (0.876)
[150]	Ethereum	Y-Y	Classification and Deep Learning: ETH Tracking Tree Method, LightGBM, LSTM, RF, **XGBoost**	Accuracy (0.95), F1 (0.9542), Precision (0.961), Recall (0.9469)

[102]	Ethereum	Y-N	Classification: DeepWalk, **EGAT**, GAT, GCN, Graph2vec, GraphSage, MLP, Node2vec, Softmax, Sub2vec	Accuracy (0.981), F1 (0.979), Precision (0.966), Recall (0.993)
[103]	Ethereum	Y-N	Classification and Graph Learning: Adam Optimizer, GCN, Graph Isomorphism Network, Graph2Vec, **GraphSAGE**, SF	Accuracy (0.9878), AUROC (0.9876), F1 (0.9878), Precision (0.9878), Recall (0.9880)
[159]	Ethereum	Y-N	Classification: DT, KNN, MLP; and Deep Learning: **CNN**	Accuracy (0.8754), F1 (0.85), Precision (0.8768), Recall (0.8448)
[115]	Bitcoin and Ethereum	N-N	Classification: LR, **RF**, **SVM**	Accuracy (0.987-0.834), F1 (0.994-0.909), Recall (0.897-0.835)
[104]	Ethereum	N-N	Classification: 48 Consolidated, C4.5 DT, Eth-PSD, Fast DT, JRip, NB Tree, OneR, PART decision List	Accuracy (0.9776), F1 (0.97), FPR (0.01), Precision (0.97), Recall (0.97), ROC (0.97), Time taken to build a model (0.03)
[55]	Steem	N-N	Classification: **AdaBoost**, DT, LightGBM, Linear Support Vector, MLP, **RF with Entropy**, **RF with Gini**, XGBoost	Accuracy (0.9268), F1 (0.8832), Precision (0.8512), Recall (0.9250)
[142]	Bitcoin	Y-N	Classification: AdaBoost, Bayes Network, NB, **RF**; and Clustering: k-Means	FPR (0.007), Number of Correctly Classified Instances (0.9948), Number of Incorrectly Classified Instances (0.0052), PRC (1.0), Precision (0.995), Recall (0.995), ROC (1.0), TPR (0.995)
[129]	Bitcoin	Y-N	Classification: AdaBoost, CatBoost, DT, KNN, LightGBM, LGBM, LR, MLP, **RF**, SVC, XGB, **XGBoost**	Accuracy (0.9921), F1 (0.957), Index of Balanced Accuracy (0.9599), Precision (0.997), Recall (0.922)
[130]	Bitcoin	Y-N	Classification: **AdaBoost**, KNN, LOF, Mahalanobis Distance-Based Method, MLP, OCSVM, **RF**, SVM	Accuracy (0.995), F1 (0.959), Precision (0.981), Recall (0.97)

Table 10: Papers Addressing Anomaly Detection

6.3 Cryptocurrency Price Prediction

We found thirty papers addressing cryptocurrency price prediction.

The great majority of these studies focused on Bitcoin. Several authors applied a regression and/or deep learning, using different sets of algorithms: (i) ANN, LSTM, and RF [163]; Multiplayer Dynamic Game Model and SVM [164]; Bayesian NN, LR, and SVR [165]; Graph Chainlets and RF [166]; Bayesian Regression and a GLM/Random forest [167]; and a GRU, GRU-Dropout, GRU-Dropout-GRU, LSTM, and NN [168].

The authors included the following features into their models: technology and economic factors [163, 165, 167, 168], game theory-related factors [164]; and graph chainlets [166].

The datasets used in these papers covered different periods of time: three different periods in [163] (specifically: (i) August 1, 2011 - December 31, 2013; (ii) August 1, 2013 - December 21, 2014; (iii) July 1, 2014 - December 31, 2017; (iv) July 1, 2015 - July 31, 2018); from September 13, 2011, to July 21, 2017 [165]; from 2008 to 2009 [166]; and from January 1, 2010 to June 30, 2019 [168]

Six papers applied a time series analysis to Bitcoin data, with different periods of time: from October 2013 - March 2021 [169]; from January 2013–May 2017 [170]; from September 4, 2011 to February 28, 2014 [171]; from October 27, 2014 to January 12, 2015 [172]; until December 31, 2014 [173]. In [174], the authors studied two periods: (i) January 1, 2011 to December 31, 2013; (ii) July 1, 2013 to December 31, 2014. The features used in these papers include both technology factors and economic factors.

Nine papers addressed the price prediction problem from a classification and/or deep learning perspective, and tried to predict the direction of the price movement instead of the price point. The algorithms used in these papers are: Linear Discriminant Analysis, LR, LSTM, Quadratic Discriminant Analysis, RF, SVM, XGBoost [175]; Ensemble, Feedforward NN, GB, GRU, LSTM, RNN, RF [176]; a regression for classification task [177]; DT, KNN, Linear Discriminant Analysis, LR, Quadratic Discriminant Analysis, RF, SVM, XGBoost [178]; CNB, CNN, CNN-LSTM, CNN-GRU, DT, GRU, LR, LSTM, SVM, RF [179]; BPNN, PCA-SVR, SDAE, and SVR [180]; CNN, Combinations of CNNs and RNNs, DNN, DRN, Ensemble Models, RNN and LSTM [181]; DNDT, DRCNN, DSVR [182]; and CNN [183]. In order to train and test these models, the authors used various sets of features: technology features, economic features and attention features [175, 176, 178, 179, 182]; technology features and economic features [180, 181, 183]; and Bitcoin daily transaction graphs [177]. Finally, the authors used data covering various periods of time: from July 2013 - December 2019 [180]; from November 29, 2011 to December 31, 2018 [181]; from 2011 to 2019, with a quarterly frequency of data [182]; and from 2015 [183]. In [176], the authors used a dataset covering the period from March 4, 2019 to December 10, 2019. Two papers used two datasets: [175] ((i) February 2 2017 to February 1 2019, and (ii) July 17 2017 to January 17 2018); and [178] ((i) data and Bitcoin daily price from January 1, 2017, to December 31, 2019; and (ii) Bitcoin 5-min interval price for the period November 2, 2016 to June 11, 2018). The authors in [179] used a dataset of less than 100,000 data points.

Four papers applied both a classification and a regression to address the cryptocurrency price prediction problem. The algorithms used in the papers we analyzed here include: ANN, Ensemble, RNN, and SVM [184]; ARIMA, LSTM, and RNN [185]; ANN, LSTM, SANN, and SVM [186]; and Deep Cross Networks, DNN, and FLRDS [187]. The datasets used in the studies consisted of various sets of features: Bitcoin price-related features and transaction fees [184]; and technology features and economic features [185, 186, 187]. The datasets used for these studies covered various numbers of periods: two periods ((i) August 19, 2013 - July 19, 2016; (ii) April 1st, 2013 - April 1st, 2017) in [184]; one period (August 19, 2013 to July 19, 2016) in [185] and (from February 2014 - September 2021) in [187]; and three periods ((i) April 1, 2013 to July 19, 2016; (ii) April 1, 2013 to April 1, 2017; (iii) April 1, 2013 to December 31, 2019) in [186].

Finally, for the Bitcoin price prediction, [188] used Multimodal Causality Testing with technology features, economic features and attention features, and data spanning from February 2018 - January 2020; while [189] used various algorithms (i.e. Multi-Window Prediction Framework, Full connected NN, and SVM). To get this result, the authors extracted transaction subgraphs and used data from April 1, 2013 to December 31, 2017.

[190] analyzed Ether price prediction, with data ranging from August 11, 2015 to November 28, 2018. They predicted the cryptocurrency price using SVM; ANN with technology features and economic features.

One paper studied price prediction on Bitcoin and Ethereum [191]. The authors used technology features and economic features as input to several regressors (ANN, Conjugate Gradient, Elastic Net, GB, LASSO, LR, LSTM, RF). They used a dataset of less than 2,000 data points covering a period from December 18, 2017 - November 30, 2020.

Finally, [52] focused on cryptocurrency price prediction on Bitcoin, Ethereum, and Ripple. The authors used a dataset consisting of more than 1,000,000 data points and composed of the technology features, economic features and attention features. They used various regressors (Conjugate Gradient Approach, Linear Regression, LSTM, regression with GB, regression with RF).

Paper	Blockchain	Data-Code	Model	Performance
[190]	Ethereum	N-N	Regression: **ANN**, SVM	MAPE (0.048), RMSE (0.068)

[188]	Bitcoin	Y-Y	Multimodal Causality Testing: Multiple-Output Convolutional Gaussian	Hypotheses Testing
[169]	Bitcoin	N-N	Time Series Analysis: VAR	Unclear
[175]	Bitcoin	N-N	Classification and Deep Learning: Linear Discriminant Analysis, LR, **LSTM**, Quadratic Discriminant Analysis, RF, SVM, **XGBoost**	Accuracy (0.672), F1 (0.776), Precision (0.817), Recall (0.840)
[163]	Bitcoin	N-N	Regression and Deep Learning: ANN, **LSTM**, RF	DA (76.5), MAE (8.7512), MAPE (2.2793), RMSE (12.0632)
[176]	Bitcoin	N-N	Classification and Deep Learning: Ensemble, Feedforward NN, GB, GRU, **LSTM**, RF, RNN	Accuracy (0.56)
[184]	Bitcoin	N-N	Classification: ANN, **Ensemble**, SVM; and Regression: ANN, RNN, **SVM**,	Accuracy (0.6291), AUC (0.58), MAE (6.7), MAPE (1.14%), RMSE (12.12)
[180]	Bitcoin	N-N	Deep Learning: BPNN, PCA-SVR, **SDAE**, SVR	DA (0.5985), MAPE (0.1019), RMSE (160.63)
[52]	Bitcoin, Ethereum, and Ripple	N-N	Regression: ANN, Combination Forecasts, Elastic Net, GB, **LAD**, LASSO, Monitoring Forecasts, **Rank** Regression, RF, Shrinkage Estimators	Accuracy (0.561-0.538-0.557), CSSED, MAD (2.68-3.53-3.18), R^2 (0.0269-0.0171-0.0212)
[164]	Bitcoin	N-N	Regression: **Multiplayer Dynamic Game Model**, **SVM**	Accuracy (0.642), Precision (0.877), Sensitivity (0.439), Specificity (0.623)
[177]	Bitcoin	N-N	Classification: Regression for classification task	AUC PR (0.51), AUC ROC (0.73)
[165]	Bitcoin	N-N	Regression: **Bayesian NN**, Linear Regression, SVR	MAPE (0.0198-0.6302), RMSE (0.0244-0.5114)
[170]	Bitcoin	N-N	Time Series Analysis: Bayesian Structural Time Series	MAE (12.139), MSE (457.65), sMAPE (2.970%)
[191]	Bitcoin and Ethereum	N-N	Regression: **Conjugate Gradient**, Linear Regression, LSTM, Regression with GB, Regression with RF	MAE (- - -), RMSE (- - -)
[181]	Bitcoin	N-N	Deep Learning: Combinations of CNNs and RNNs, CNN, **DNN**, Deep Residual Networks, Ensemble Models, Recurrent Neural Networks and LSTM, **SVM**	Accuracy (0.5306), F1 (0.67), MAPE (3.60%), Precision (0.5290), Recall (1.0), Specificity (0.5370)
[171]	Bitcoin	N-N	Time Series Analysis	Unclear
[182]	Bitcoin	N-N	Deep Learning: DNDT, **DRCNN**, DSVR	Accuracy (0.9527), MAPE (0.29), RMSE (0.66)
[174]	Bitcoin	Y-N	Time Series Analysis: Time series using ARDL Model	F-Statistics, R^2 (0.284)

[185]	Bitcoin	N-N	Classification and Deep Learning and Regression: **ARIMA**, **LSTM**, **RNN**	Accuracy (0.5278), Precision (1.0), RMSE (5.45%), Sensitivity (0.4040), Specificity (1.0)
[186]	Bitcoin	N-N	Classification and Deep Learning and Regression: ANN, **LSTM**, **SANN**, SVM	Accuracy (0.64), AUC (0.66), F1 (0.71), MAE (1.24), MAPE (0.52%), RMSE (1.58)
[173]	Bitcoin	N-N	Time Series Analysis: Vector Autoregression	P-Value
[166]	Bitcoin	Y-Y	Regression: **Graph Chainlets**, RF	RMSE
[167]	Bitcoin	N-N	Regression: Bayesian Regression, GLM/RF	Unclear
[168]	Bitcoin	N-N	Regression and Deep Learning: GRU, **GRU-Dropout**, GRU-Dropout-GRU, LSTM, Neural Network	RMSE (0.017)
[183]	Bitcoin	N-N	Deep Learning: CNN	Unclear
[172]	Bitcoin	N-N	Time Series Analysis: OLS	p-Value
[189]	Bitcoin	Y-N	Unclear: Full connected NN , **Multi-Window Prediction Framework**, SVM	MAPE (1.69%)
[187]	Bitcoin	N-N	Classification and Regression: DCN, DNN, **Hybrid Model**	Loss Ratio (0.0), MAE (9.96% - 1707.42), ROI (11%), Sharpe ratio (1.03), Total profit (USD 65,043.99), Volatility (0.07), Win Ratio (1.0), Win–loss Ratio (-)
[178]	Bitcoin	N-N	Classification: DT, KNN, **Linear Discriminant Analysis**, **LR**, Quadratic Discriminant Analysis, RF, **SVM**, XGBoost	Accuracy (0.648), Confusion Matrix, F1 (0.63), Precision (0.71), Recall (1.0)
[179]	Bitcoin	Y-Y	Classification and Deep Learning: **CNN**, **CNN-GRU**, **CNN-LSTM**, Complement NB, DT, GRU, LR, LSTM, RF, SVM	Accuracy (0.6086), F1, Precision (0.60), Recall (0.60)

Table 11: Papers Addressing Cryptocurrency Price Prediction

6.4 Performance Prediction

Seven papers in this study addressed a performance prediction problem, using a classification task [192, 193, 194], a regression task [54], a classification and deep learning tasks [195, 196], or a time series analysis [197].

Two papers proposed a solution for gas price prediction on Ethereum. [196] used the gas price spanning from October 10, 2020 to October 24, 2020, while [195] used gas-related features spanning from March 17, 2022 to April 13, 2022.

The five other papers focused on the transactions: transaction throughput prediction on Hyperledger Fabric [54], transaction confirmation time prediction on Ethereum [192, 193, 194], and transaction fees prediction [197]. In order to address these topics, the authors used: transaction latency, send rate, transaction throughput, and error [54]; gas-related features and transaction-time related features [192]; transaction-specific features, block-

and network-specific features [193]; and cryptocurrency prices-related features and block- and network-specific features [197].

All datasets used in these papers consisted of at least more than 10,000 data points. They covered various periods, ranging from before November 2018 until April 2022. August 2019.

Paper	Blockchain	Data-Code	Model	Performance
[54]	Hyperledger Fabric	Y-N	Regression: ANN	MAD (0.250), MSE (6.701), RMSE (2.716)
[192]	Ethereum	N-N	Classification: **MLP**, NB, RF	Accuracy (0.8361), Cohen's Kappa (0.7877)
[197]	Ethereum	Y-N	Time Series Analysis: Granger causality	p-Value
[193]	Ethereum	N-N	Classification: Ensemble Approach, KNN, MLP, **RF**, SVM,	Accuracy (0.9018), F1 (0.897), Macro F1, Precision (0.896), Recall (0.896), ROC (0.936)
[195]	Ethereum	N-N	Classification and Deep Learning: **LSTM**, **XBoost**	MAE (0.064), RMSE (0.108), R^2 (0.962)
[196]	Ethereum	Y-Y	Classification and Deep Learning: **GRU**, **LSTM**, Prophet, RNN	MAE (0.063), MSE (0.008), R^2 (0.896), RMSE (0.088)
[194]	Ethereum	Y-Y	Classification: **DT**, LR, **RF**, SVM	Accuracy (0.98272), AUC-ROC (0.873668), F1 (0.674454), F2 (0.617612), Matthews Correlation Coefficient (0.702714), Precision (0.797683), Recall (0.973890), TNR (0.995), TPR (0.974)

Table 12: Papers Addressing Performance Prediction

6.5 Smart Contract Vulnerability Detection

In our studies, we found twelve papers addressing smart contract vulnerability detection, assessment or classification on Ethereum. All papers used classifiers and/or deep learning models and reported various performance measures.

In the papers in our study, the authors experimented with a set of classifiers and/or deep learning algorithms: (i) DR-GCN, Eth2Vec, MODNN, SoliAudit [198]; (i) CNN, DT, KNN, LR, RF, SVM [199]; (ii) DT, NN, RF, SVM [200]; (iii) Vanilla-RNN, LSTM, BLSTM, BLSTM-ATT [201]; (iv) KNN, RF, SVM [202]; (v) AdaBoost, KNN, RF, SVM, XGBoost [203]. Also, multiple authors proposed a novel classification algorithm: the Average Stochastic Gradient Descent Weighted Dropped Long Short Term Memory [204], Bytecode matching [205], Peculiar [206], DeeSCVHunter [207], SmartEmbed [208], and Eth2Vec [209]. They usually compared the performance of their solution with baseline models.

As far as the features fed to the models are concerned, the opcode is a popular feature [198, 199, 204]. Furthermore, the authors in [200] extracted 17 features from the smart contract code: (i) features representing the execution path, and (ii) features representing heuristic guesses of the complexity of the code. In [209], the authors used the same features, except for the hexadecimal address. Other features used in the papers we studied include: contract snippets [201], bigram features from simplified opcodes [202, 203], bytecode [205], crucial data flow graph [206], and vulnerability candidate slice [207].

Except for the study by [201], all papers used datasets with more than 10,000 data points. Also, no authors reported a dataset spanning after 2018.

Paper	Blockchain	Data-Code	Model	Performance
[198]	Ethereum	Y-Y	Classification and Deep Learning: **DR-GCN**, Eth2Vec, **MODNN**, SoliAudit	Accuracy, Euclidian Distance, F1 (0.9628), FN, FP, Fowlkes and Mallows Index, Loss function, Precision (0.9651), Recall (1.0), TN, TP
[204]	Ethereum	Y-N	Deep Learning: **Average Stochastic Gradient Descent Weighted Dropped Long Short Term Memory**	Accuracy (0.913), F1 (0.952), Precision (0.944), Recall (0.979)
[205]	Ethereum	N-N	Classification: Bytecode matching	FNR (0.1429), FPR (0.0), Precision (0.9195)
[199]	Ethereum	N-N	Classification and Deep Learning: CNN, DT, KNN, **LR**, RF, SVM	Accuracy (0.973), F1 (0.904), Precision (0.929), Recall (0.882)
[200]	Ethereum	N-N	Classification: DT, NN, RF, SVM	Accuracy, F1, FN, FP, Precision, Recall, TN, TP
[201]	Ethereum	N-Y	Classification and Deep Learning: BLSTM, **BLSTM-ATT**, LSTM, Vanilla-RNN	Accuracy (0.8847), AUC, F1 (0.8826), FPR (0.0857), Precision (0.8850), Recall, ROC Curve
[202]	Ethereum	N-N	Classification: KNN, **RF**, SVM	F1 (0.98), Macro-F1 (0.9303), Micro-F1 (0.9698), ROC
[203]	Ethereum	N-N	Classification: AdaBoost, KNN, RF, SVM, **XGBoost**	F1 (0.99), Macro-F1 (0.9641), Micro-F1 (0.9798), ROC
[206]	Ethereum	Y-Y	Classification: Peculiar	F1 (0.9210), Precision (0.9180), Recall (0.9240)
[207]	Ethereum	Y-N	Classification: **DeeSCVHunter**	Accuracy (0.9302), F1 (0.8687), Precision (0.9070), Recall (0.8346)
[208]	Ethereum	Y-Y	Deep Learning: Sequence to sequence recurrent autoencoder	-
[209]	Ethereum	Y-Y	Classification: **Eth2Vec**, NNN, SVM	F1 (0.575), Precision (0.77), Recall (0.507)

Table 13: Papers Addressing Smart Contract Vulnerability Detection

6.6 Other

We found three papers that do not fit the identified categories above. Specifically, [49] addressed behavior pattern clustering. The authors used a dataset of less than 2,000 data points. Next, [50] proposed a solution for smart contracts labeling on Ethereum, with a dataset of less than 1,000 data points. The authors used k-medoids and Affinity Propagation algorithms to obtain seven clusters. Finally, in [51] , the authors applied a clustering algorithm on a dataset of less than 100,000 data points. The goal was to perform some data analysis on the EOS blockchain.

Paper	Blockchain	Data-Code	Model	Performance
[49]	Unclear	N-N	Clustering: **BPC**, BPC with Random Cluster Center Initialization	Precision (0.7426)
[50]	Ethereum	N-N	Clustering: Affinity Propagation, k-Medoids	Frequency distribution
[51]	EOSIO	Y-N	Clustering	Average Shortest Path Length, Clustering coefficient (0.448), Degree Distribution

Table 14: Papers Addressing Other Use Cases

7 Discussion & Conclusion

7.1 Major Findings

In this work, we conducted a systematic mapping study on Machine Learning techniques applied to blockchain data. We analyzed 159 articles, selected and classified them according to various dimensions. In order to perform this study, we followed the most widely accepted guidelines in the literature and gave an overview of the current research in the given area. This structured methodology allowed us to extract key information and address the four main research questions. We also identified the gaps in the existing research works and recognized future research directions.

In this study, we selected the most relevant and important publications by applying inclusion and exclusion criteria in a process consisting of 6 phases, while querying in the most widely used scientific databases in these fields i.e. Google Scholar, Springer, and ScienceDirect. The publication forums of the studies, as well as the distribution of the studies by publication type were extensively analyzed.

Followingly, the studies were classified according to four different perspectives:

1. **Domain & Use Case** with the major use cases being address classification, anomaly detection, cryptocurrency price prediction, performance prediction, smart contract vulnerability detection. The majority of the studies we considered here addressed the problems of anomaly detection.

2. **Blockchain Platform** with the majority of studies focusing on Bitcoin and Ethereum data, while some research teams focused on a combination of blockchains.

3. **Data** with detailed analysis on the blockchain and external data sources as well as the size of datasets examined by the different studies to draw interesting results. It was inferred that the majority of studies were based on datasets of more than 1,000,000 data points and while some datasets were made available by the authors or were available by default, the majority of studies did not share the data they used.

4. **Machine Learning Models** applied to blockchain data such as classification, clustering, deep learning, graph learning, regression, time series analysis, or a combination of the above, with classification being the most widely used technique. Regarding the machine learning workflow followed in the different studies, some preprocessing techniques were commonly employed such as data preprocessing, feature extraction, and algorithm selection. On the subject of the specific algorithms, Random Forest and the Support Vector Machine were the most favored ones and the most commonly utilized evaluation metrics across studies were Accuracy, Precision, Recall, F-Score, and ROC Curve.

7.2 Challenges and Future Research Directions

As blockchains are increasingly popular, their size increases significantly depending on the number of transactions, the block size, the frequency of the block creation, and the additional data stored e.g. Ethereum smart contract events and metadata. Larger data size, which currently exceeds hundred of Gigabytes for the most popular blockchains, pose challenges in terms of storage, and computational requirements in applying machine learning to blockchain data and fully leverage the potential of machine learning algorithms in this context.

Furthermore, to exploit the significant amount of valuable information stored in the different smart contracts and Decentralized Applications requires an additional notable effort to preprocess and often to develop solutions in order to extract it from blocks and transactions. This challenge requires further attention and it is indicative that there is an initial effort in this direction for Ethereum DApps [119] and DeFi [210] with many potentials by taking also into consideration the interoperability between different blockchains and external data sources.

While some research works such as [116] [135] published their underlying datasets and acted as a reference point and a comparison baseline, most works are not making their dataset/code available and as a result, there is a lack of standardized evaluation frameworks and benchmarks. An additional challenge would be the constant update of such benchmarks with the latest block data and the domain's changing patterns. As an example in the domain of Anomaly Detection new malicious accounts, illicit transactions, Ponzi schemes based on smart contracts, and phishing activities constantly emerge, based on novel patterns and mechanisms and the efficient proposed algorithms should be able to identify the most recent malicious activities. This lack of data sharing is a common problem in academia, and many reasons explain this issue, such as insufficient time, lack of funding, lack of skills, or authors' attitudes. Various mechanisms could be put in place in order to promote or facilitate data sharing, including: explicit data sharing policies from journals, support from authors' institutions, better infrastructure/data repositories, or incentives for sharing [211, 212, 213, 214].

Finally, in relation to the points raised above, blockchain is a fast evolving technology: new blockchains, new protocols, new DApps, new use cases, and new interactions with other technologies (blockchain and IoT, blockchain and AI) emerge constantly. Being able to store and process the growing volumes of data is crucial, as well as being able to compare past phenomena with the current ones. The latter would be made possible with proper data sharing.

7.3 Conclusion

In summary, this study provided detailed insights into the research works on applying machine learning to blockchain data. As the adoption of blockchains continues to grow, new technical solutions are integrated and new services emerge. Future research needs to take into consideration such aspects in order to better understand the research landscape. Novel research is needed to propose standardized frameworks across the different use cases analyzed in the context of this work. As significant growth in machine learning research is noticed and the proposal of innovative ML algorithms is observed, future research is also required to explore their tailoring, customization and potential for the unique features of blockchain problems and data.

Acknowledgment

This work was supported by J.P.Morgan Faculty Research Awards 2022 and NSF 1932220.

References

[1] S. Keele *et al.*, "Guidelines for performing systematic literature reviews in software engineering," 2007.

[2] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," in *12th International Conference on Evaluation and Assessment in Software Engineering (EASE) 12*, pp. 1–10, 2008.

[3] Z. A. Siddiqui and M. Haroon, "Application of artificial intelligence and machine learning in blockchain technology," in *Artificial Intelligence and Machine Learning for EDGE Computing*, pp. 169–185, Elsevier, 2022.

[4] X. A. Inbaraj and T. R. Chaitanya, "Need to know about combined technologies of blockchain and machine learning," in *Handbook of research on blockchain technology*, pp. 417–432, Elsevier, 2020.

[5] A. Aoun, A. Ilinca, M. Ghandour, and H. Ibrahim, "A review of industry 4.0 characteristics and challenges, with potential improvements using blockchain technology," *Computers & Industrial Engineering*, vol. 162, p. 107746, 2021.

[6] Y. Wu, Z. Wang, Y. Ma, and V. C. Leung, "Deep reinforcement learning for blockchain in industrial iot: A survey," *Computer Networks*, vol. 191, p. 108004, 2021.

[7] K. Liu, Z. Yan, X. Liang, R. Kantola, and C. Hu, "A survey on blockchain-enabled federated learning and its prospects with digital twin," *Digital Communications and Networks*, 2022.

[8] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, "A survey on security in internet of things with a focus on the impact of emerging technologies," *Internet of Things*, vol. 19, p. 100564, 2022.

[9] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, “Survey on iot security: Challenges and solution using machine learning, artificial intelligence and blockchain technology,” *Internet of Things*, vol. 11, p. 100227, 2020.

[10] W. Hua, Y. Chen, M. Qadrdan, J. Jiang, H. Sun, and J. Wu, “Applications of blockchain and artificial intelligence technologies for enabling prosumers in smart grids: A review,” *Renewable and Sustainable Energy Reviews*, vol. 161, p. 112308, 2022.

[11] H. Han, R. K. Shiwakoti, R. Jarvis, C. Mordi, and D. Botchie, “Accounting and auditing with blockchain technology and artificial intelligence: A literature review,” *International Journal of Accounting Information Systems*, vol. 48, p. 100598, 2023.

[12] A. S. Cheng, Q. Guan, Y. Su, P. Zhou, and Y. Zeng, “Integration of machine learning and blockchain technology in the healthcare field: a literature review and implications for cancer care,” *Asia-Pacific Journal of Oncology Nursing*, vol. 8, no. 6, pp. 720–724, 2021.

[13] Y.-S. Ren, C.-Q. Ma, X.-L. Kong, K. Baltas, and Q. Zureigat, “Past, present, and future of the application of machine learning in cryptocurrency research,” *Research in International Business and Finance*, vol. 63, p. 101799, 2022.

[14] C. Bai and J. Sarkis, “A critical review of formal analytical modeling for blockchain technology in production, operations, and supply chains: Harnessing progress for future potential,” *International Journal of Production Economics*, p. 108636, 2022.

[15] A. Miglani and N. Kumar, “Blockchain management and machine learning adaptation for iot environment in 5g and beyond networks: A systematic review,” *Computer Communications*, vol. 178, pp. 37–63, 2021.

[16] C.-Y. Lin, H.-K. Liao, and F.-C. Tsai, “A systematic review of detecting illicit bitcoin transactions,” *Procedia Computer Science*, vol. 207, pp. 3217–3225, 2022.

[17] M. U. Hassan, M. H. Rehmani, and J. Chen, “Anomaly detection in blockchain networks: A comprehensive survey,” *IEEE Communications Surveys & Tutorials*, 2022.

[18] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *Decentralized business review*, p. 21260, 2008.

[19] V. Buterin *et al.*, “A next-generation smart contract and decentralized application platform,”

[20] G. Palaiokrassas, P. Skoufis, O. Voutyras, T. Kawasaki, M. Gallissot, R. Azzabi, A. Tsuge, A. Litke, T. Okoshi, J. Nakazawa, *et al.*, “Combining blockchains, smart contracts, and complex sensors management platform for hyper-connected smartcities: An iot data marketplace use case,” *Computers*, vol. 10, no. 10, p. 133, 2021.

[21] G. Palaiokrassas, A. Litke, G. Fragkos, V. Papaefthymiou, and T. Varvarigou, “Deploying blockchains for a new paradigm of media experience,” in *Economics of Grids, Clouds, Systems, and Services: 15th International Conference, GECON 2018, Pisa, Italy, September 18–20, 2018, Proceedings 15*, pp. 234–242, Springer, 2019.

[22] M. M. Queiroz, R. Telles, and S. H. Bonilla, “Blockchain and supply chain management integration: a systematic review of the literature,” *Supply chain management: An international journal*, vol. 25, no. 2, pp. 241–254, 2020.

[23] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, “Blockchain technology in healthcare: a systematic review,” in *Healthcare*, vol. 7, p. 56, MDPI, 2019.

[24] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, “Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” *Renewable and sustainable energy reviews*, vol. 100, pp. 143–174, 2019.

[25] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, “Sok: Decentralized finance (defi),” *arXiv preprint arXiv:2101.08778*, 2021.

[26] L. M. Bach, B. Mihaljevic, and M. Zagar, “Comparative analysis of blockchain consensus algorithms,” in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1545–1550, 2018.

[27] M. I. Jordan and T. M. Mitchell, “Machine learning: Trends, perspectives, and prospects,” *Science*, vol. 349, no. 6245, pp. 255–260, 2015.

[28] M. P. Deisenroth, A. A. Faisal, and C. S. Ong, *Mathematics for machine learning.* Cambridge University Press, 2020.

[29] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. Leung, "Blockchain and machine learning for communications and networking systems," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1392–1431, 2020.

[30] J. E. Van Engelen and H. H. Hoos, "A survey on semi-supervised learning," *Machine learning*, vol. 109, no. 2, pp. 373–440, 2020.

[31] A. Abdelmaboud, D. N. Jawawi, I. Ghani, A. Elsafi, and B. Kitchenham, "Quality of service approaches in cloud computing: A systematic mapping study," *Journal of Systems and Software*, vol. 101, pp. 159–179, 2015.

[32] C.-W. Tsai, Y.-P. Chen, T.-C. Tang, and Y.-C. Luo, "An efficient parallel machine learning-based blockchain framework," *ICT Express*, vol. 7, no. 3, pp. 300–307, 2021.

[33] Z. Wang, J. Liu, Q. Wu, Y. Zhang, H. Yu, and Z. Zhou, "An analytic evaluation for the impact of uncle blocks by selfish and stubborn mining in an imperfect ethereum network," *Computers & Security*, vol. 87, p. 101581, 2019.

[34] A. Kalafatelis, K. Panagos, A. E. Giannopoulos, S. T. Spantideas, N. C. Kapsalis, M. Touloupou, E. Kapassa, L. Katelaris, P. Christodoulou, K. Christodoulou, *et al.*, "Island: An interlinked semantically-enriched blockchain data framework," in *International Conference on the Economics of Grids, Clouds, Systems, and Services*, pp. 207–214, Springer, 2021.

[35] O. Pal, S. Singh, and V. Kumar, "Blockchain network: Performance optimization," in *Applications of Artificial Intelligence and Machine Learning*, pp. 677–686, Springer, 2022.

[36] L. Ouyang, W. Zhang, and F.-Y. Wang, "Intelligent contracts: Making smart contracts smart for blockchain intelligence," *Computers and Electrical Engineering*, vol. 104, p. 108421, 2022.

[37] J. You, "Curvetime: A blockchain framework for artificial intelligence computation," *Software Impacts*, vol. 13, p. 100314, 2022.

[38] G. S. Atsalakis, I. G. Atsalaki, F. Pasiouras, and C. Zopounidis, "Bitcoin price forecasting with neuro-fuzzy techniques," *European Journal of Operational Research*, vol. 276, no. 2, pp. 770–780, 2019.

[39] S. Lahmiri and S. Bekiros, "Intelligent forecasting with machine learning trading systems in chaotic intraday bitcoin market," *Chaos, Solitons & Fractals*, vol. 133, p. 109641, 2020.

[40] V. Manahov and A. Urquhart, "The efficiency of bitcoin: A strongly typed genetic programming approach to smart electronic bitcoin markets," *International Review of Financial Analysis*, vol. 73, p. 101629, 2021.

[41] P. Ciaian, M. Rajcaniova, *et al.*, "Virtual relationships: Short-and long-run evidence from bitcoin and altcoin markets," *Journal of International Financial Markets, Institutions and Money*, vol. 52, pp. 173–195, 2018.

[42] S. Lahmiri and S. Bekiros, "Big data analytics using multi-fractal wavelet leaders in high-frequency bitcoin markets," *Chaos, Solitons & Fractals*, vol. 131, p. 109472, 2020.

[43] F. Liu, Y. Li, B. Li, J. Li, and H. Xie, "Bitcoin transaction strategy construction based on deep reinforcement learning," *Applied Soft Computing*, vol. 113, p. 107952, 2021.

[44] R. K. Rathore, D. Mishra, P. S. Mehra, O. Pal, A. S. HASHIM, A. Shapi'i, T. Ciano, and M. Shutaywi, "Real-world model for bitcoin price prediction," *Information Processing & Management*, vol. 59, no. 4, p. 102968, 2022.

[45] V. Veselỳ and M. Žádník, "How to detect cryptocurrency miners? by traffic forensics!," *Digital Investigation*, vol. 31, p. 100884, 2019.

[46] N. Sundareswaran and S. Sasirekha, "Packet filtering mechanism to defend against ddos attack in blockchain network," in *Evolutionary Computing and Mobile Sustainable Networks*, pp. 201–214, Springer, 2022.

[47] W. Zheng, Z. Zheng, H.-N. Dai, X. Chen, and P. Zheng, "Xblock-eos: Extracting and exploring blockchain data from eosio," *Information Processing & Management*, vol. 58, no. 3, p. 102477, 2021.

[48] V. Kanth, J. McEachen, and M. Tummala, “Parameter identification for malicious transaction detection in blockchain protocols,” in *International Congress on Blockchain and Applications*, pp. 54–63, Springer, 2022.

[49] B. Huang, Z. Liu, J. Chen, A. Liu, Q. Liu, and Q. He, “Behavior pattern clustering in blockchain networks,” *Multimedia Tools and Applications*, vol. 76, pp. 20099–20110, 2017.

[50] R. Norvill, B. B. F. Pontiveros, R. State, I. Awan, and A. Cullen, “Automated labeling of unknown contracts in ethereum,” in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–6, IEEE, 2017.

[51] W. Song, W. Zhang, L. Zhai, L. Liu, J. Wang, S. Huang, and B. Li, “Eos. io blockchain data analysis,” *The Journal of Supercomputing*, vol. 78, no. 4, pp. 5974–6005, 2022.

[52] J. Yae and G. Z. Tian, “Out-of-sample forecasting of cryptocurrency returns: A comprehensive comparison of predictors and algorithms,” *Physica A: Statistical Mechanics and its Applications*, vol. 598, p. 127379, 2022.

[53] J. Shen, J. Zhou, Y. Xie, S. Yu, and Q. Xuan, “Identity inference on blockchain using graph neural network,” in *International Conference on Blockchain and Trustworthy Systems*, pp. 3–17, Springer, 2021.

[54] L. Hang, I. Ullah, J. Yang, and C. Chen, “An improved kalman filter using ann-based learning module to predict transaction throughput of blockchain network in clinical trials,” *Peer-to-Peer Networking and Applications*, pp. 1–18, 2022.

[55] T. Kim, H. Shin, H. J. Hwang, and S. Jeong, “Posting bot detection on blockchain-based social media platform using machine learning techniques,” in *Proceedings of the International AAAI Conference on Web and Social Media*, vol. 15, pp. 303–314, 2021.

[56] P. L. Juhász, J. Stéger, D. Kondor, and G. Vattay, “A bayesian approach to identify bitcoin users,” *PloS one*, vol. 13, no. 12, p. e0207000, 2018.

[57] S. Ranshous, C. A. Joslyn, S. Kreyling, K. Nowak, N. F. Samatova, C. L. West, and S. Winters, “Exchange pattern mining in the bitcoin transaction directed hypergraph,” in *Financial Cryptography and Data Security: FC 2017 International Workshops, WAHC, BITCOIN, VOTING, WTSC, and TA, Sliema, Malta, April 7, 2017, Revised Selected Papers 21*, pp. 248–263, Springer, 2017.

[58] J. V. Monaco, “Identifying bitcoin users by transaction behavior,” in *Biometric and surveillance technology for human and activity identification XII*, vol. 9457, pp. 25–39, SPIE, 2015.

[59] H. H. Sun Yin, K. Langenheldt, M. Harlev, R. R. Mukkamala, and R. Vatrapu, “Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain,” *Journal of Management Information Systems*, vol. 36, no. 1, pp. 37–73, 2019.

[60] M. A. Harlev, H. Sun Yin, K. C. Langenheldt, R. Mukkamala, and R. Vatrapu, “Breaking bad: De-anonymising entity types on the bitcoin blockchain using supervised machine learning,” in *Proceedings of the 51st Hawaii international conference on system sciences*, 2018.

[61] C. Kang, C. Lee, K. Ko, J. Woo, and J. W.-K. Hong, “De-anonymization of the bitcoin network using address clustering,” in *Blockchain and Trustworthy Systems: Second International Conference, BlockSys 2020, Dali, China, August 6–7, 2020, Revised Selected Papers 2*, pp. 489–501, Springer, 2020.

[62] C. Remy, B. Rym, and L. Matthieu, “Tracking bitcoin users activity using community detection on a network of weak signals,” in *Complex Networks & Their Applications VI: Proceedings of Complex Networks 2017 (The Sixth International Conference on Complex Networks and Their Applications)*, pp. 166–177, Springer, 2018.

[63] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, “A fistful of bitcoins: characterizing payments among men with no names,” in *Proceedings of the 2013 conference on Internet measurement conference*, pp. 127–140, 2013.

[64] B. Zheng, L. Zhu, M. Shen, X. Du, J. Yang, F. Gao, Y. Li, C. Zhang, S. Liu, and S. Yin, “Malicious bitcoin transaction tracing using incidence relation clustering,” in *Mobile Networks and Management: 9th International Conference, MONAMI 2017, Melbourne, Australia, December 13-15, 2017, Proceedings 9*, pp. 313–323, Springer, 2018.

[65] B. Zheng, L. Zhu, M. Shen, X. Du, and M. Guizani, “Identifying the vulnerabilities of bitcoin anonymous mechanism based on address clustering,” *Science China Information Sciences*, vol. 63, pp. 1–15, 2020.

[66] R. R. Tubino, C. Robardet, and R. Cazabet, “Towards a better identification of bitcoin actors by supervised learning,” *Data & Knowledge Engineering*, vol. 142, p. 102094, 2022.

[67] W. Shao, H. Li, M. Chen, C. Jia, C. Liu, and Z. Wang, “Identifying bitcoin users using deep neural network,” in *Algorithms and Architectures for Parallel Processing: 18th International Conference, ICA3PP 2018, Guangzhou, China, November 15-17, 2018, Proceedings, Part IV 18*, pp. 178–192, Springer, 2018.

[68] Z. Zhang, T. Zhou, and Z. Xie, “Bitscope: Scaling bitcoin address de-anonymization using multi-resolution clustering,” in *Proceedings of the 51st Hawaii International Conference on System Sciences*, pp. 1–11, 2018.

[69] X. Xueshuo, W. Jiming, Y. Junyi, F. Yaozheng, L. Ye, L. Tao, and W. Guiling, “Awap: Adaptive weighted attribute propagation enhanced community detection model for bitcoin de-anonymization,” *Applied Soft Computing*, vol. 109, p. 107507, 2021.

[70] C. Lee, S. Maharjan, K. Ko, J. Woo, and J. W.-K. Hong, “Machine learning based bitcoin address classification,” in *Blockchain and Trustworthy Systems: Second International Conference, BlockSys 2020, Dali, China, August 6–7, 2020, Revised Selected Papers 2*, pp. 517–531, Springer, 2020.

[71] J. Liang, L. Li, W. Chen, and D. Zeng, “Targeted addresses identification for bitcoin with network representation learning,” in *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pp. 158–160, IEEE, 2019.

[72] Y.-J. Lin, P.-W. Wu, C.-H. Hsu, I.-P. Tu, and S.-w. Liao, “An evaluation of bitcoin address classification based on transaction history summarization,” in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 302–310, IEEE, 2019.

[73] K. Toyoda, T. Ohtsuki, and P. T. Mathiopoulos, “Multi-class bitcoin-enabled service identification based on transaction history summarization,” in *2018 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*, pp. 1153–1160, IEEE, 2018.

[74] F. Zola, M. Eguimendia, J. L. Bruse, and R. O. Urrutia, “Cascading machine learning to attack bitcoin anonymity,” in *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 10–17, IEEE, 2019.

[75] H. S. Yin and R. Vatrapu, “A first estimation of the proportion of cybercriminal entities in the bitcoin ecosystem using supervised machine learning,” in *2017 IEEE International Conference on Big Data (Big Data)*, pp. 3690–3699, IEEE, 2017.

[76] J. A. Blanco and A. J. Tallón-Ballesteros, “Supervised machine learning techniques in the bitcoin transactions. a case of ransomware classification,” in *16th International Conference on Soft Computing Models in Industrial and Environmental Applications (SOCO 2021)*, pp. 803–810, Springer, 2022.

[77] X. Sun, T. Yang, and B. Hu, “Lstm-tc: Bitcoin coin mixing detection method with a high recall,” *Applied Intelligence*, vol. 52, no. 1, pp. 780–793, 2022.

[78] F. Béres *et al.*, “Blockchain is watching you: Profiling and deanonymizing ethereum users,” in *2021 IEEE Int. DAPPS Conference*, pp. 69–78, 2021.

[79] J. Liu, J. Zheng, J. Wu, and Z. Zheng, “Fa-gnn: Filter and augment graph neural networks for account classification in ethereum,” *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 4, pp. 2579–2588, 2022.

[80] H. Tang, Y. Jiao, B. Huang, C. Lin, S. Goyal, and B. Wang, “Learning to classify blockchain peers according to their behavior sequences,” *IEEE Access*, vol. 6, pp. 71208–71215, 2018.

[81] M. Jourdan, S. Blandin, L. Wynter, and P. Deshpande, “Characterizing entities in the bitcoin blockchain,” in *2018 IEEE international conference on data mining workshops (ICDMW)*, pp. 55–62, IEEE, 2018.

[82] X. F. Liu, H.-H. Ren, S.-H. Liu, and X.-J. Jiang, “Characterizing key agents in the cryptocurrency economy through blockchain transaction analysis,” *EPJ Data Science*, vol. 10, no. 1, p. 21, 2021.

[83] M. Bartoletti, B. Pes, and S. Serusi, “Data mining for detecting bitcoin ponzi schemes,” in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pp. 75–84, IEEE, 2018.

[84] W. Chen, Z. Zheng, J. Cui, E. Ngai, P. Zheng, and Y. Zhou, "Detecting ponzi schemes on ethereum: Towards healthier blockchain technology," in *Proceedings of the 2018 world wide web conference*, pp. 1409–1418, 2018.

[85] 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.

[86] L. Wang, H. Cheng, Z. Zheng, A. Yang, and X. Zhu, "Ponzi scheme detection via oversampling-based long short-term memory for smart contracts," *Knowledge-Based Systems*, vol. 228, p. 107312, 2021.

[87] Y. Zhang, W. Yu, Z. Li, S. Raza, and H. Cao, "Detecting ethereum ponzi schemes based on improved lightgbm algorithm," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 2, pp. 624–637, 2021.

[88] E. Jung, M. Le Tilly, A. Gehani, and Y. Ge, "Data mining-based ethereum fraud detection," in *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 266–273, IEEE, 2019.

[89] J. Peng and G. Xiao, "Detection of smart ponzi schemes using opcode," in *Blockchain and Trustworthy Systems: Second International Conference, BlockSys 2020, Dali, China, August 6–7, 2020, Revised Selected Papers 2*, pp. 192–204, Springer, 2020.

[90] S. Fan, S. Fu, H. Xu, and X. Cheng, "Al-spsd: Anti-leakage smart ponzi schemes detection in blockchain," *Information Processing & Management*, vol. 58, no. 4, p. 102587, 2021.

[91] A. Aljofey, Q. Jiang, and Q. Qu, "A supervised learning model for detecting ponzi contracts in ethereum blockchain," in *International Conference on Big Data and Security*, pp. 657–672, Springer, 2021.

[92] W. Sun, G. Xu, Z. Yang, and Z. Chen, "Early detection of smart ponzi scheme contracts based on behavior forest similarity," in *2020 IEEE 20th International Conference on Software Quality, Reliability and Security (QRS)*, pp. 297–309, IEEE, 2020.

[93] B. Fu, X. Yu, and T. Feng, "Ct-gcn: a phishing identification model for blockchain cryptocurrency transactions," *International Journal of Information Security*, vol. 21, no. 6, pp. 1223–1232, 2022.

[94] L. Chen, J. Peng, Y. Liu, J. Li, F. Xie, and Z. Zheng, "Phishing scams detection in ethereum transaction network," *ACM Transactions on Internet Technology (TOIT)*, vol. 21, no. 1, pp. 1–16, 2020.

[95] Q. Yuan, B. Huang, J. Zhang, J. Wu, H. Zhang, and X. Zhang, "Detecting phishing scams on ethereum based on transaction records," in *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–5, IEEE, 2020.

[96] Z. Yuan, Q. Yuan, and J. Wu, "Phishing detection on ethereum via learning representation of transaction subgraphs," in *Blockchain and Trustworthy Systems: Second International Conference, BlockSys 2020, Dali, China, August 6–7, 2020, Revised Selected Papers 2*, pp. 178–191, Springer, 2020.

[97] J. Wu, Q. Yuan, D. Lin, W. You, W. Chen, C. Chen, and Z. Zheng, "Who are the phishers? phishing scam detection on ethereum via network embedding," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 2, pp. 1156–1166, 2020.

[98] Y. Xia, J. Liu, and J. Wu, "Phishing detection on ethereum via attributed ego-graph embedding," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 5, pp. 2538–2542, 2022.

[99] H. Wen, J. Fang, J. Wu, and Z. Zheng, "Transaction-based hidden strategies against general phishing detection framework on ethereum," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–5, IEEE, 2021.

[100] T. Wen, Y. Xiao, A. Wang, and H. Wang, "A novel hybrid feature fusion model for detecting phishing scam on ethereum using deep neural network," *Expert Systems with Applications*, vol. 211, p. 118463, 2023.

[101] Y. Wang, Z. Liu, J. Xu, and W. Yan, "Heterogeneous network representation learning approach for ethereum identity identification," *IEEE Transactions on Computational Social Systems*, 2022.

[102] X. Zhou, W. Yang, and X. Tian, "Detecting phishing accounts on ethereum based on transaction records and egat," *Electronics*, vol. 12, no. 4, p. 993, 2023.

[103] J. Kim, S. Lee, Y. Kim, S. Ahn, and S. Cho, "Graph learning-based blockchain phishing account detection with a heterogeneous transaction graph," *Sensors*, vol. 23, no. 1, p. 463, 2023.

[104] A. H. H. Kabla, M. Anbar, S. Manickam, and S. Karupayah, “Eth-psd: A machine learning-based phishing scam detection approach in ethereum,” *IEEE Access*, vol. 10, pp. 118043–118057, 2022.

[105] W. Chen, J. Cui, X. Guo, Z. Chen, and Y. Lu, “Misbehavior detection on blockchain data,” in *Blockchain Intelligence*, pp. 95–133, Springer, 2021.

[106] W. Chen, Y. Xu, Z. Zheng, Y. Zhou, J. E. Yang, and J. Bian, “Detecting” pump & dump schemes” on cryptocurrency market using an improved apriori algorithm,” in *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*, pp. 293–2935, IEEE, 2019.

[107] P. Monamo, V. Marivate, and B. Twala, “Unsupervised learning for robust bitcoin fraud detection,” in *2016 Information Security for South Africa (ISSA)*, pp. 129–134, IEEE, 2016.

[108] P. M. Monamo, V. Marivate, and B. Twala, “A multifaceted approach to bitcoin fraud detection: Global and local outliers,” in *2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pp. 188–194, IEEE, 2016.

[109] K. Toyoda, T. Ohtsuki, and P. T. Mathiopoulos, “Identification of high yielding investment programs in bitcoin via transactions pattern analysis,” in *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pp. 1–6, IEEE, 2017.

[110] J. Lorenz, M. I. Silva, D. Aparício, J. T. Ascensão, and P. Bizarro, “Machine learning methods to detect money laundering in the bitcoin blockchain in the presence of label scarcity,” in *Proceedings of the First ACM International Conference on AI in Finance*, pp. 1–8, 2020.

[111] A. Wahrstätter, J. Gomes, S. Khan, and D. Svetinovic, “Improving cryptocurrency crime detection: Coinjoin community detection approach,” *IEEE Transactions on Dependable and Secure Computing*, 2023.

[112] A. Aljofey, A. Rasool, Q. Jiang, and Q. Qu, “A feature-based robust method for abnormal contracts detection in ethereum blockchain,” *Electronics*, vol. 11, no. 18, p. 2937, 2022.

[113] T. Ashfaq, R. Khalid, A. S. Yahaya, S. Aslam, A. T. Azar, S. Alsafari, and I. A. Hameed, “A machine learning and blockchain based efficient fraud detection mechanism,” *Sensors*, vol. 22, no. 19, p. 7162, 2022.

[114] H. Hall, P. Baiz, and P. Nadler, “Efficient analysis of transactional data using graph convolutional networks,” in *Machine Learning and Principles and Practice of Knowledge Discovery in Databases: International Workshops of ECML PKDD 2021, Virtual Event, September 13-17, 2021, Proceedings, Part II*, pp. 210–225, Springer, 2022.

[115] Y. Elmougy and O. Manzi, “Anomaly detection on bitcoin, ethereum networks using gpu-accelerated machine learning methods,” in *2021 31st International Conference on Computer Theory and Applications (ICCTA)*, pp. 166–171, IEEE, 2021.

[116] M. Weber, G. Domeniconi, J. Chen, D. K. I. Weidele, C. Bellei, T. Robinson, and C. E. Leiserson, “Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics,” *arXiv preprint arXiv:1908.02591*, 2019.

[117] C. Lee, S. Maharjan, K. Ko, and J. W.-K. Hong, “Toward detecting illegal transactions on bitcoin using machine-learning methods,” in *Blockchain and Trustworthy Systems: First International Conference, BlockSys 2019, Guangzhou, China, December 7–8, 2019, Proceedings 1*, pp. 520–533, Springer, 2020.

[118] H. Han, R. Wang, Y. Chen, K. Xie, and K. Zhang, “Research on abnormal transaction detection method for blockchain,” in *International Conference on Blockchain and Trustworthy Systems*, pp. 223–236, Springer, 2022.

[119] T. Min and W. Cai, “Portrait of decentralized application users: an overview based on large-scale ethereum data,” *CCF Transactions on Pervasive Computing and Interaction*, vol. 4, no. 2, pp. 124–141, 2022.

[120] V. Patel, S. Rajasegarar, L. Pan, J. Liu, and L. Zhu, “Evangcn: Evolving graph deep neural network based anomaly detection in blockchain,” in *Advanced Data Mining and Applications: 18th International Conference, ADMA 2022, Brisbane, QLD, Australia, November 28–30, 2022, Proceedings, Part I*, pp. 444–456, Springer, 2022.

[121] V. Patel, L. Pan, and S. Rajasegarar, “Graph deep learning based anomaly detection in ethereum blockchain network,” in *International Conference on Network and System Security*, pp. 132–148, Springer, 2020.

[122] S. Al-E'mari, M. Anbar, Y. Sanjalawe, and S. Manickam, "A labeled transactions-based dataset on the ethereum network," in *Advances in Cyber Security: Second International Conference, ACeS 2020, Penang, Malaysia, December 8-9, 2020, Revised Selected Papers 2*, pp. 61–79, Springer, 2021.

[123] L. Liu, W.-T. Tsai, M. Z. A. Bhuiyan, H. Peng, and M. Liu, "Blockchain-enabled fraud discovery through abnormal smart contract detection on ethereum," *Future Generation Computer Systems*, vol. 128, pp. 158–166, 2022.

[124] F. Scicchitano, A. Liguori, M. Guarascio, E. Ritacco, and G. Manco, "A deep learning approach for detecting security attacks on blockchain.," in *ITASEC*, pp. 212–222, 2020.

[125] T. Hu, X. Liu, T. Chen, X. Zhang, X. Huang, W. Niu, J. Lu, K. Zhou, and Y. Liu, "Transaction-based classification and detection approach for ethereum smart contract," *Information Processing & Management*, vol. 58, no. 2, p. 102462, 2021.

[126] B. Podgorelec, M. Turkanović, and S. Karakatič, "A machine learning-based method for automated blockchain transaction signing including personalized anomaly detection," *Sensors*, vol. 20, no. 1, p. 147, 2019.

[127] H. Baek, J. Oh, C. Y. Kim, and K. Lee, "A model for detecting cryptocurrency transactions with discernible purpose," in *2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 713–717, IEEE, 2019.

[128] I. Alarab and S. Prakoonwit, "Effect of data resampling on feature importance in imbalanced blockchain data: Comparison studies of resampling techniques," *Data Science and Management*, 2022.

[129] E. V. Feldman, A. N. Ruchay, V. K. Matveeva, and V. D. Samsonova, "Bitcoin abnormal transaction detection based on machine learning," in *Recent Trends in Analysis of Images, Social Networks and Texts: 9th International Conference, AIST 2020, Skolkovo, Moscow, Russia, October 15–16, 2020 Revised Supplementary Proceedings 9*, pp. 205–215, Springer, 2021.

[130] B. Chen, F. Wei, and C. Gu, "Bitcoin theft detection based on supervised machine learning algorithms," *Security and Communication Networks*, vol. 2021, pp. 1–10, 2021.

[131] M. Rwibasira and R. Suchithra, "Adobsvm: Anomaly detection on block chain using support vector machine," *Measurement: Sensors*, vol. 24, p. 100503, 2022.

[132] R. Zhang, G. Zhang, L. Liu, C. Wang, and S. Wan, "Anomaly detection in bitcoin information networks with multi-constrained meta path," *Journal of Systems Architecture*, vol. 110, p. 101829, 2020.

[133] C. Zhao and Y. Guan, "A graph-based investigation of bitcoin transactions," in *Advances in Digital Forensics XI: 11th IFIP WG 11.9 International Conference, Orlando, FL, USA, January 26-28, 2015, Revised Selected Papers 11*, pp. 79–95, Springer, 2015.

[134] M. Deepa and D. Akila, "Cost-effective anomaly detection for blockchain transactions using unsupervised learning," in *Intelligent Computing and Innovation on Data Science*, pp. 445–453, Springer, 2021.

[135] S. Farrugia, J. Ellul, and G. Azzopardi, "Detection of illicit accounts over the ethereum blockchain," *Expert Systems with Applications*, vol. 150, p. 113318, 2020.

[136] J. Wu, J. Liu, W. Chen, H. Huang, Z. Zheng, and Y. Zhang, "Detecting mixing services via mining bitcoin transaction network with hybrid motifs," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 4, pp. 2237–2249, 2021.

[137] Y. Li, Y. Cai, H. Tian, G. Xue, and Z. Zheng, "Identifying illicit addresses in bitcoin network," in *Blockchain and Trustworthy Systems: Second International Conference, BlockSys 2020, Dali, China, August 6–7, 2020, Revised Selected Papers 2*, pp. 99–111, Springer, 2020.

[138] K. Kanemura, K. Toyoda, and T. Ohtsuki, "Identification of darknet markets' bitcoin addresses by voting per-address classification results," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 154–158, IEEE, 2019.

[139] A. Elbaghdadi, S. Mezroui, and A. El Oualkadi, "Svm: an approach to detect illicit transaction in the bitcoin network," in *Innovations in Smart Cities Applications Volume 4: The Proceedings of the 5th International Conference on Smart City Applications*, pp. 1130–1141, Springer, 2021.

[140] I. Alarab and S. Prakoonwit, "Graph-based lstm for anti-money laundering: Experimenting temporal graph convolutional network with bitcoin data," *Neural Processing Letters*, pp. 1–19, 2022.

[141] S. Eloul, S. J. Moran, and J. Mendel, “Improving streaming cryptocurrency transaction classification via biased sampling and graph feedback,” in *Annual Computer Security Applications Conference*, pp. 761–772, 2021.

[142] D. Boughaci and A. A. Alkhawaldeh, “Enhancing the security of financial transactions in blockchain by using machine learning techniques: Towards a sophisticated security tool for banking and finance,” in *2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH)*, pp. 110–115, IEEE, 2020.

[143] A. Ahmed, “Anti-money laundering recognition through the gradient boosting classifier,” *Academy of Accountingand Financial Studies Journal*, vol. 25, no. 5, 2021.

[144] I. Alarab, S. Prakoonwit, and M. I. Nacer, “Competence of graph convolutional networks for anti-money laundering in bitcoin blockchain,” in *Proceedings of the 2020 5th international conference on machine learning technologies*, pp. 23–27, 2020.

[145] H. Zheng, B. Wen, and Y. Li, “Recognize illegal transactions in the bitcoin network using graph attention with dikw,” in *2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys)*, pp. 2118–2123, IEEE, 2021.

[146] M. Ostapowicz and K. Żbikowski, “Detecting fraudulent accounts on blockchain: a supervised approach,” in *International Conference on Web Information Systems Engineering*, pp. 18–31, Springer, 2020.

[147] H. Sun, N. Ruan, and H. Liu, “Ethereum analysis via node clustering,” in *Network and System Security: 13th International Conference, NSS 2019, Sapporo, Japan, December 15–18, 2019, Proceedings 13*, pp. 114–129, Springer, 2019.

[148] D. Vassallo, V. Vella, and J. Ellul, “Application of gradient boosting algorithms for anti-money laundering in cryptocurrencies,” *SN Computer Science*, vol. 2, pp. 1–15, 2021.

[149] B. Kılıç, A. Sen, and C. Özturan, “Fraud detection in blockchains using machine learning,” in *2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)*, pp. 214–218, IEEE, 2022.

[150] Z. Yuan, T. Yang, and J. Cao, “Eth-tt: A novel approach for detecting ethereum malicious accounts,” in *Artificial Intelligence: Second CAAI International Conference, CICAI 2022, Beijing, China, August 27–28, 2022, Revised Selected Papers, Part II*, pp. 84–94, Springer, 2023.

[151] F. Poursafaei, G. B. Hamad, and Z. Zilic, “Detecting malicious ethereum entities via application of machine learning classification,” in *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pp. 120–127, IEEE, 2020.

[152] R. F. Ibrahim, A. M. Elian, and M. Ababneh, “Illicit account detection in the ethereum blockchain using machine learning,” in *2021 International Conference on Information Technology (ICIT)*, pp. 488–493, IEEE, 2021.

[153] R. M. Aziz, M. F. Baluch, S. Patel, and A. H. Ganie, “Lgbm: a machine learning approach for ethereum fraud detection,” *International Journal of Information Technology*, pp. 1–11, 2022.

[154] J. Zhou, S. Yan, and J. Zhang, “Prediction and analysis of illegal accounts on ethereum based on catboost algorithm,” in *2022 International Conference on Big Data, Information and Computer Network (BDICN)*, pp. 63–67, IEEE, 2022.

[155] A. Bella Baci, K. Brousmiche, I. Amal, F. Abdelhédi, and L. Rigaud, “Detecting illicit ethereum accounts based on their transaction history and properties and using machine learning,” in *The International Conference on Deep Learning, Big Data and Blockchain (DBB 2022)*, pp. 97–108, Springer, 2022.

[156] F. Poursafaei, R. Rabbany, and Z. Zilic, “Sigtran: Signature vectors for detecting illicit activities in blockchain transaction networks,” in *Pacific-Asia Conference on Knowledge Discovery and Data Mining*, pp. 27–39, Springer, 2021.

[157] T. Chen, Z. Li, Y. Zhu, J. Chen, X. Luo, J. C.-S. Lui, X. Lin, and X. Zhang, “Understanding ethereum via graph analysis,” *ACM Transactions on Internet Technology (TOIT)*, vol. 20, no. 2, pp. 1–32, 2020.

[158] D. Saveetha and G. Maragatham, “Design of blockchain enabled intrusion detection model for detecting security attacks using deep learning,” *Pattern Recognition Letters*, vol. 153, pp. 24–28, 2022.

[159] O. Sanda, M. Pavlidis, S. Seraj, and N. Polatidis, "Long-range attack detection on permissionless blockchains using deep learning," *Expert Systems with Applications*, vol. 218, p. 119606, 2023.

[160] M. Caprolu, S. Raponi, G. Oligeri, and R. Di Pietro, "Cryptomining makes noise: Detecting cryptojacking via machine learning," *Computer Communications*, vol. 171, pp. 126–139, 2021.

[161] S. Boudko, H. Abie, M. Boscolo, and D. Ferrario, "Predictive analytics service for security of blockchain and peer-to-peer payment solutions," in *Information Science and Applications*, pp. 71–81, Springer, 2021.

[162] B. B. Zarpelão, R. S. Miani, and M. Rajarajan, "Detection of bitcoin-based botnets using a one-class classifier," in *Information Security Theory and Practice: 12th IFIP WG 11.2 International Conference, WISTP 2018, Brussels, Belgium, December 10–11, 2018, Revised Selected Papers 12*, pp. 174–189, Springer, 2019.

[163] W. Chen, H. Xu, L. Jia, and Y. Gao, "Machine learning model for bitcoin exchange rate prediction using economic and technology determinants," *International Journal of Forecasting*, vol. 37, no. 1, pp. 28–43, 2021.

[164] G. Yan, S. Wang, S. Li, and B. Lu, "Multi-player dynamic game model for bitcoin transaction bidding prediction," *The North American Journal of Economics and Finance*, vol. 60, p. 101631, 2022.

[165] H. Jang and J. Lee, "An empirical study on modeling and prediction of bitcoin prices with bayesian neural networks based on blockchain information," *Ieee Access*, vol. 6, pp. 5427–5437, 2017.

[166] C. G. Akcora, A. K. Dey, Y. R. Gel, and M. Kantarcioglu, "Forecasting bitcoin price with graph chainlets," in *Advances in Knowledge Discovery and Data Mining: 22nd Pacific-Asia Conference, PAKDD 2018, Melbourne, VIC, Australia, June 3-6, 2018, Proceedings, Part III 22*, pp. 765–776, Springer, 2018.

[167] S. Velankar, S. Valecha, and S. Maji, "Bitcoin price prediction using machine learning," in *2018 20th International Conference on Advanced Communication Technology (ICACT)*, pp. 144–147, IEEE, 2018.

[168] A. Dutta, S. Kumar, and M. Basu, "A gated recurrent unit approach to bitcoin price prediction," *Journal of Risk and Financial Management*, vol. 13, no. 2, p. 23, 2020.

[169] C. Cai, W. Li, H. Han, and M. Liu, "Risk scenario-based value estimation of bitcoin," *Procedia Computer Science*, vol. 199, pp. 1198–1204, 2022.

[170] O. Poyser, "Exploring the dynamics of bitcoin's price: a bayesian structural time series approach," *Eurasian Economic Review*, vol. 9, no. 1, pp. 29–60, 2019.

[171] L. Kristoufek, "What are the main drivers of the bitcoin price? evidence from wavelet coherence analysis," *PloS one*, vol. 10, no. 4, p. e0123923, 2015.

[172] I. Georgoula, D. Pournarakis, C. Bilanakos, D. Sotiropoulos, and G. M. Giaglis, "Using time-series and sentiment analysis to detect the determinants of bitcoin prices," *Available at SSRN 2607167*, 2015.

[173] S. Y. Yang and J. Kim, "Bitcoin market return and volatility forecasting using transaction network flow properties," in *2015 IEEE Symposium Series on Computational Intelligence*, pp. 1778–1785, IEEE, 2015.

[174] X. Li and C. A. Wang, "The technology and economic determinants of cryptocurrency exchange rates: The case of bitcoin," *Decision support systems*, vol. 95, pp. 49–60, 2017.

[175] Z. Chen, C. Li, and W. Sun, "Bitcoin price prediction using machine learning: An approach to sample dimension engineering," *Journal of Computational and Applied Mathematics*, vol. 365, p. 112395, 2020.

[176] P. Jaquart, D. Dann, and C. Weinhardt, "Short-term bitcoin market prediction via machine learning," *The journal of finance and data science*, vol. 7, pp. 45–66, 2021.

[177] N. Antulov-Fantulin, D. Tolic, M. Piskorec, Z. Ce, and I. Vodenska, "Inferring short-term volatility indicators from the bitcoin blockchain," in *International Conference on Complex Networks and their Applications*, pp. 508–520, Springer, 2018.

[178] S. Ranjan, P. Kayal, and M. Saraf, "Bitcoin price prediction: A machine learning sample dimension approach," *Computational Economics*, pp. 1–20, 2022.

[179] A. M. Kanji, I. Chaudhary, R. L. Shankar, and G. Srinivasa, "Predicting the price direction of bitcoin using twitter data and machine learning," in *2022 IEEE 2nd International Conference on Data Science and Computer Application (ICDSCA)*, pp. 46–52, IEEE, 2022.

[180] M. Liu, G. Li, J. Li, X. Zhu, and Y. Yao, "Forecasting the price of bitcoin using deep learning," *Finance research letters*, vol. 40, p. 101755, 2021.

[181] S. Ji, J. Kim, and H. Im, "A comparative study of bitcoin price prediction using deep learning," *Mathematics*, vol. 7, no. 10, p. 898, 2019.

[182] P. Lamothe-Fernández, D. Alaminos, P. Lamothe-López, and M. A. Fernández-Gámez, "Deep learning methods for modeling bitcoin price," *Mathematics*, vol. 8, no. 8, p. 1245, 2020.

[183] S. Yogeshwaran, M. J. Kaur, and P. Maheshwari, "Project based learning: predicting bitcoin prices using deep learning," in *2019 IEEE Global Engineering Education Conference (EDUCON)*, pp. 1449–1454, IEEE, 2019.

[184] D. C. Mallqui and R. A. Fernandes, "Predicting the direction, maximum, minimum and closing prices of daily bitcoin exchange rate using machine learning techniques," *Applied Soft Computing*, vol. 75, pp. 596–606, 2019.

[185] S. McNally, J. Roche, and S. Caton, "Predicting the price of bitcoin using machine learning," in *2018 26th euromicro international conference on parallel, distributed and network-based processing (PDP)*, pp. 339–343, IEEE, 2018.

[186] M. Mudassir, S. Bennbaia, D. Unal, and M. Hammoudeh, "Time-series forecasting of bitcoin prices using high-dimensional features: a machine learning approach," *Neural computing and applications*, pp. 1–15, 2020.

[187] P. K. Nagula and C. Alexakis, "A new hybrid machine learning model for predicting the bitcoin (btc-usd) price," *Journal of Behavioral and Experimental Finance*, vol. 36, p. 100741, 2022.

[188] I. Chalkiadakis, A. Zaremba, G. W. Peters, and M. J. Chantler, "On-chain analytics for sentiment-driven statistical causality in cryptocurrencies," *Blockchain: Research and Applications*, vol. 3, no. 2, p. 100063, 2022.

[189] X. Li and L. Du, "Bitcoin daily price prediction through understanding blockchain transaction pattern with machine learning methods," *Journal of Combinatorial Optimization*, vol. 45, no. 1, p. 4, 2023.

[190] H.-M. Kim, G.-W. Bock, and G. Lee, "Predicting ethereum prices with machine learning based on blockchain information," *Expert Systems with Applications*, vol. 184, p. 115480, 2021.

[191] M. Saad, J. Choi, D. Nyang, J. Kim, and A. Mohaisen, "Toward characterizing blockchain-based cryptocurrencies for highly accurate predictions," *IEEE Systems Journal*, vol. 14, no. 1, pp. 321–332, 2019.

[192] H. J. Singh and A. S. Hafid, "Prediction of transaction confirmation time in ethereum blockchain using machine learning," in *International Congress on Blockchain and Applications*, pp. 126–133, Springer, 2019.

[193] A. M. Fajge, S. Goswami, A. Srivastava, and R. Halder, "Wait or reset gas price?: A machine learning-based prediction model for ethereum transactions' waiting time," in *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 1153–1160, IEEE, 2021.

[194] V. C. Oliveira, J. Almeida Valadares, J. E. A. Sousa, A. Borges Vieira, H. S. Bernardino, S. Moraes Villela, and G. Dias Goncalves, "Analyzing transaction confirmation in ethereum using machine learning techniques," *ACM SIGMETRICS Performance Evaluation Review*, vol. 48, no. 4, pp. 12–15, 2021.

[195] D. Lan, H. Wang, C. Yin, L. Zhou, C. Ge, and X. Lu, "Gas price prediction based on machine learning combined with ethereum mempool," in *2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, pp. 346–354, IEEE, 2022.

[196] R. Mars, A. Abid, S. Cheikhrouhou, and S. Kallel, "A machine learning approach for gas price prediction in ethereum blockchain," in *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, pp. 156–165, IEEE, 2021.

[197] G. A. Pierro and H. Rocha, "The influence factors on ethereum transaction fees," in *2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, pp. 24–31, IEEE, 2019.

[198] L. Zhang, J. Wang, W. Wang, Z. Jin, Y. Su, and H. Chen, "Smart contract vulnerability detection combined with multi-objective detection," *Computer Networks*, vol. 217, p. 109289, 2022.

[199] J.-W. Liao, T.-T. Tsai, C.-K. He, and C.-W. Tien, “Soliaudit: Smart contract vulnerability assessment based on machine learning and fuzz testing,” in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, pp. 458–465, IEEE, 2019.

[200] P. Momeni, Y. Wang, and R. Samavi, “Machine learning model for smart contracts security analysis,” in *2019 17th International Conference on Privacy, Security and Trust (PST)*, pp. 1–6, IEEE, 2019.

[201] P. Qian, Z. Liu, Q. He, R. Zimmermann, and X. Wang, “Towards automated reentrancy detection for smart contracts based on sequential models,” *IEEE Access*, vol. 8, pp. 19685–19695, 2020.

[202] J. Song, H. He, Z. Lv, C. Su, G. Xu, and W. Wang, “An efficient vulnerability detection model for ethereum smart contracts,” in *Network and System Security: 13th International Conference, NSS 2019, Sapporo, Japan, December 15–18, 2019, Proceedings 13*, pp. 433–442, Springer, 2019.

[203] W. Wang, J. Song, G. Xu, Y. Li, H. Wang, and C. Su, “Contractward: Automated vulnerability detection models for ethereum smart contracts,” *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1133–1144, 2020.

[204] A. K. Gogineni, S. Swayamjyoti, D. Sahoo, K. K. Sahu, and R. Kishore, “Multi-class classification of vulnerabilities in smart contracts using awd-lstm, with pre-trained encoder inspired from natural language processing,” *IOP SciNotes*, vol. 1, no. 3, p. 035002, 2020.

[205] J. Huang, S. Han, W. You, W. Shi, B. Liang, J. Wu, and Y. Wu, “Hunting vulnerable smart contracts via graph embedding based bytecode matching,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2144–2156, 2021.

[206] H. Wu, Z. Zhang, S. Wang, Y. Lei, B. Lin, Y. Qin, H. Zhang, and X. Mao, “Peculiar: Smart contract vulnerability detection based on crucial data flow graph and pre-training techniques,” in *2021 IEEE 32nd International Symposium on Software Reliability Engineering (ISSRE)*, pp. 378–389, IEEE, 2021.

[207] X. Yu, H. Zhao, B. Hou, Z. Ying, and B. Wu, “Deescvhunter: A deep learning-based framework for smart contract vulnerability detection,” in *2021 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–8, IEEE, 2021.

[208] Z. Gao, “When deep learning meets smart contracts,” in *Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering*, pp. 1400–1402, 2020.

[209] N. Ashizawa, N. Yanai, J. P. Cruz, and S. Okamura, “Eth2vec: Learning contract-wide code representations for vulnerability detection on ethereum smart contracts,” *Blockchain: Research and Applications*, vol. 3, no. 4, p. 100101, 2022.

[210] G. Palaiokrassas, S. Scherrers, I. Ofeidis, and L. Tassiulas, “Leveraging machine learning for multichain defi fraud detection,” *arXiv preprint arXiv:2306.07972*, 2023.

[211] C. Tenopir, S. Allard, K. Douglass, A. U. Aydinoglu, L. Wu, E. Read, M. Manoff, and M. Frame, “Data sharing by scientists: practices and perceptions,” *PloS one*, vol. 6, no. 6, p. e21101, 2011.

[212] Y. Kim and P. Zhang, “Understanding data sharing behaviors of stem researchers: The roles of attitudes, norms, and data repositories,” *Library & Information Science Research*, vol. 37, no. 3, pp. 189–200, 2015.

[213] W. Zenk-Möltgen, E. Akdeniz, A. Katsanidou, V. Naßhoven, and E. Balaban, “Factors influencing the data sharing behavior of researchers in sociology and political science,” *Journal of documentation*, vol. 74, no. 5, pp. 1053–1073, 2018.

[214] L. Perrier, E. Blondal, and H. MacDonald, “The views, perspectives, and experiences of academic researchers with data sharing and reuse: A meta-synthesis,” *PloS one*, vol. 15, no. 2, p. e0229182, 2020.