information

MDPI

Article

Scams and Solutions in Cryptocurrencies—A Survey Analyzing Existing Machine Learning Models

Lakshmi Priya Krishnan *, Iman Vakilinia, Sandeep Reddivari and Sanjay Ahuja

School of Computing, University of North Florida, Jacksonville, FL 32224, USA
* Correspondence: lakshmipriya.krishnan@unf.edu

Abstract: With the emergence of cryptocurrencies and Blockchain technology, the financial sector is turning its gaze toward this latest wave. The use of cryptocurrencies is becoming very common for multiple services. Food chains, network service providers, tech companies, grocery stores, and so many other services accept cryptocurrency as a mode of payment and give several incentives for people who pay using them. Despite this tremendous success, cryptocurrencies have opened the door to fraudulent activities such as Ponzi schemes, HYIPs (high-yield investment programs), money laundering, and much more, which has led to the loss of several millions of dollars. Over the decade, solutions using several machine learning algorithms have been proposed to detect these felonious activities. The objective of this paper is to survey these models, the datasets used, and the underlying technology. This study will identify highly efficient models, evaluate their performances, and compile the extracted features, which can serve as a benchmark for future research. Fraudulent activities and their characteristics have been exposed in this survey. We have identified the gaps in the existing models and propose improvement ideas that can detect scams early.

Keywords: cryptocurrencies; scams; blockchain; machine learning; fraud detection

Citation: Krishnan, L.P.; Vakilinia, I.; Reddivari, S.; Ahuja, S. Scams and Solutions in Cryptocurrencies—A Survey Analyzing Existing Machine Learning Models. *Information* **2023**, *14*, 171. https://doi.org/10.3390/info14030171

Academic Editors: Georgios Siolas, Georgios Alexandridis, Paraskevi Tzouveli and Kun She

Received: 21 December 2022
Revised: 3 March 2023
Accepted: 4 March 2023
Published: 8 March 2023

1. Introduction

Over the past decade, Blockchain and cryptocurrencies have turned the outlook of investments, transactions, and in fact the entire financial sector. The very first whitepaper introducing a new currency and its network [1] was introduced in the market in November 2008 and the first transaction using Bitcoin was done in January 2009. As of February 2022, there are more than 10,300 cryptocurrencies that have come into being, which shows that the technology has gained popularity in terms of every aspect such as new coins getting introduced every few days, the number of transactions reaching millions, acceptance of cryptocurrencies in exchange for services, etc. As proof for this claim, the value of 1BTC has increased from $0 in 2009 to $20,144.44 as of 5 October 2022 [2]. Historical statistics show that the Bitcoin value has peaked at $62,000 in October 2021. In a similar fashion, the second-generation cryptocurrency Ethereum is growing extensively. Statistics reveal that there are more than 250,000 confirmed transactions of Bitcoin and more than 1,130,000 confirmed transactions of Ethereum daily [3]. The top 20 cryptocurrencies make up close to 90% of the total market.

In the right hands, cryptocurrencies have grown in terms of their value and have expanded their utility. Despite this success, some characteristics of cryptocurrencies attract felonious activities, which has resulted in the loss of several millions of dollars and personal identity. According to a report released by Federal Trade Commission [4], since the start of 2021 more than 46,000 people have lost over $1 billion in cryptocurrency scams. Alongside the technologies growth, scam rates have also increased dramatically. This report also states that the scam reports and losses have raised close to sixty times from 2018 to 2021. These scams are categorized by experts into several types such as Ponzi schemes, pump and dumps, money laundering, rug pulls, HYIPs (high-yield investment programs), hacking,

phishing, and initial coin offering (ICO) scams. In recent times, crypto scams have been reported to have started with an ad, post, or message on a social media platform. Investment scams attract naïve investors with false promises of high returns.

Resources talk about how new ICOs are introduced frequently, and the success rates of new startups which raise investment in the form of cryptocurrencies, are increasing [5]. The need for detecting the scams and safeguarding wealth is highly important as cryptocurrency is replacing fiat [6] in different services. Research works overtime have proposed detection techniques using various models and a variety of approaches. In our survey, we propose to study existing models, evaluate their efficiencies, and compile the set of features these models have exploited to detect these scams.

Before going forward to look at these models, the need to understand the characteristics of the public blockchain (this survey is focused on public blockchain technology) that attract scammers is very crucial. While trying to understand this new wave of technology, we have examined "decentralized", "pseudonym", "public records", "digital money", "secured wallets", "digital signatures", "identity by addresses", and many other terminologies. This enriched glossary makes up the blockchain. The fact that blockchain technology is decentralized and covers the identity of the user behind an address attracts scams and felonious activities.

Machine learning models that use different algorithms have been used to detect scam activities. Supervised, unsupervised, and many others such as ensemble learning and active learning models are developed by different research works to produce accurate results in identifying them. Most of the papers identify these scams as classification problems and try to classify the transactions into valid and scam related transactions, while few methods try to classify them into more labels. Research to identify malicious websites, social media posts, and fake portfolios have also attempted to provide a solution to these scams. The contribution of this survey is to analyze these techniques, this research, and these data to produce a performance analysis and a compilation for further research.

The rates at which the scammers cheat investors and lure money is increasing alarmingly. Governments, financial institutions, and investment advising agencies are trying to bring solutions, but the knowledge and understanding of blockchain technology and cryptocurrencies is inadequate among officials and investors. This work also tries to expose these efforts and provide an overview of how to secure these crypto-wallets.

In our research, we have considered different machine learning models that have worked in detecting various types of scams. For our performance analysis, we have categorized each work into a category of scams it is trying to catch. The papers we have considered have used transactional, account, and smart contract features from a dataset of cryptocurrency transactions and smart contracts. As mentioned, our research methodology categorizes the models based on their scam type and focuses on the models' performance by analyzing their accuracy, F1 score, precision, and recall. We compare existing works that use different machine learning models on different datasets for the primary reason that each of these models is aimed at identifying scams in cryptocurrencies, and the success rate of each depends on how accurate and efficient they are at achieving it.

The rest of this survey is organized in the following way:

- Section 2 explains the underlying technology of blockchain; provides background information, mainly on different types of cryptocurrency scams; and lists examples from the past.
- Section 3 talks about related surveys and existing detection techniques , which were referred to perform analysis.
- Section 4 covers all of the analysis performed to compare models, the datasets used, and the features extracted from detection models that aimed to address different types of scams.
- Section 5 lists the observations from the analysis of our survey and identifies the best performing models under various conditions.

- Section 6 concludes the survey with all of the understanding and the contributions this survey produces for further research.

2. Background

Cryptocurrencies and blockchain technology are revolutionizing the global economy in this digital era. The introduction of email changed the way the world communicates. In the same way, digital currencies and wallets have dramatically changed the way the world operates. Transactions, exchanges, and services now rely on and prefer digital currencies over traditional money. One important reason behind this is the decentralization and no third-party involvement that blockchain technology and digital currencies offer [7]. Blockchain is a peer-to-peer network that acts as a public ledger for keeping logs of transactions and any other activities. This technology serves as the neural network of cryptocurrencies and is widely used for its three most valuable characteristics: decentralization, immutability, and pseudonymity [8].

While the heart of this survey is to examine cryptocurrency scams and analyze the solutions proposed to detect them, understanding the fundamental concepts and the workings of blockchain and cryptocurrencies is very critical. One primary advantage that scammers have when defrauding users is users' lack of knowledge of how the system works. Blockchain technology is a novel record system to store information that cannot be tampered with as once a record is created it is copied across all the nodes in a network with an immutable digital signature of users. Transactions in a blockchain happen in a sequence that reflects the model and layers of a network. The process of transaction happens in the following sequence [9]:

- Signing: When a user sends money (cryptocurrency) from his wallet, a message is created with the sender's address, the receiver's address, and the amount of money. The wallet adds a digital signature that is unique and depends upon the public and private keys of the user. A block is created after the reception and collection of multiple messages.
- Broadcasting: This block is then broadcast to every node for validation.
- Confirmation: The nodes validate the transaction; the block is added to the chain and the entire network is updated with the status.

The concept of proof of work [6] comes into play in the confirmation stage, where nodes are rewarded for validating the transaction.

The first cryptocurrency, Bitcoin, has proved to be a very successful application of blockchain technology. Several new coins have been created for multiple purposes and are being used by a diversity of services. According to a report by coindesk.com [10], the blockchain market size for retail is expected to reach $4.6 billion by 2028. Not only are big corporations moving toward digital decentralized currency but several startups and medium-sized businesses are also attracted to this. Apart from Bitcoin, there are other cryptocurrencies such as Ethereum, Tether, and U.S. Dollar Coin (USDC) whose values are dramatically increasing. According to a report by Forbes, there are more than 20,000 cryptocurrency projects with values $952 billion. As of 30 September 2022, the market capitalization of Bitcoin and Ethereum is $377 billion and $165 billion, respectively [11].

With the increasing use of digital and crypto wallets, it is very crucial to understand the differences between traditional currencies and crypto coins. There are five notable differences [12], which will provide a better understanding of the use of cryptocurrencies.

- Firstly, Bitcoins or any cryptocurrencies are not controlled by a central authority such as governments or banks.
- The original identity of any cryptocurrency user can be hidden behind addresses, whereas the users are always accountable in traditional currencies.
- There is a limited number of coins, which are generally declared by the creator, instead of in traditional cash where the central authority can decide to produce more and more.

- Cryptocurrency is open-source, by which the source code of the coin or the logic is available publicly, which is not available in most traditional systems.
- Finally, cryptocurrency itself has no value, and its value decreases or increases based on usage. However, the value of a traditional currency is always endorsed by fiat.

It is evident from these differences that cryptocurrencies will continue to gain popularity and be used for multiple services. Knowing the ins and outs of this technology is crucial as it is gaining popularity. Let us look at some key concepts that will help researchers, investors, and developers who look forward to engaging with this technology. These concepts will also aid in understanding scams better because scammers exploit the lack of information on them.

- Smart contract: The introduction of smart contracts in Ethereum is one major reason for the increase in new projects and investment opportunities using cryptocurrencies. A smart contract is a program that consists of an agreement between two or more parties on a blockchain, which is immutable. These smart contracts do not require a third-party middleman, which reduces additional expenses. They work like an intelligent agent and even automate the process of transferring money to accounts based on pre-defined conditions. These contracts generally have two attributes—value and state—and they mostly use if–then statements as triggering conditions [13]. These contracts are deployed to blockchain renders transactions traceable, transparent, and irreversible.
- Initial Coin Offering (ICO): The ICO provides a way for companies to raise money to launch a new coin, app, or service. Interested investors can purchase a cryptocurrency token issued by a company through an initial coin offering. Depending on the product or service the company is offering, the token may have some utility or represent a stake in the firm. Initial coin offerings are a popular way to raise funds for products and services usually related to cryptocurrency [14].
- Whitepaper: While introducing a new coin or project, the creators release documents called a whitepaper. This whitepaper is a collection of technical, legal, and marketing information [15]. It serves as a road map for the investors while trying to understand the working and goals of a project.
- Mining: The process of producing units of cryptocurrency through some kind of effort is called mining. The effort is required because it ensures that people cannot create an infinite number of cryptocurrencies, which would reduce their value [6]. Mining also includes other processes such as validating cryptocurrency transactions on blockchain networks and adding them to the distributed ledger. Mining usually involves using computer hardware to solve a hash with trillions of possible combinations. Miners who work on this charge transaction fees as a reward for confirming transactions.
- Proof-of-Work: Proof-of-Work is a term that accounts for the work done by miners to confirm transactions in the network. Adding a block to the blockchain requires the hashing of a block, as well as time and computing power. The effort taken for this process, and efforts taken to solve hashes to create new coins, is referred to as proof-of-work.
- Double Spending: In traditional cryptocurrencies, when a user spends a particular amount for a service, they cannot spend the same cash for a different service. When it comes to cryptocurrency, the same coin can be copied multiple times and used for different purposes. This serious issue is known as double spending. The first whitepaper proposing Bitcoin [1] solved this issue using a consensus mechanism of confirming transactions by multiple nodes in a network.
- Gas: As mentioned above, miners charge transaction fees for confirming transactions. In Ethereum, this fee is referred to as gas [16]. It is important to always check for enough gas before committing a transaction because transactions can be regarded as invalid if the user does not have enough gas left in the account.
- Wallets: A wallet is a storage location or device for securing cryptocurrencies securely. Wallets are of two types: hot wallets and cold wallets. Hot wallets are online locations

generally offered by crypto exchange platforms or third parties with a private key, and cold wallets are physical storage such as flash drive or a hard drive to store crypto assets [16] .

- Bubble: A bubble is an economic cycle that is characterized by the rapid escalation of market value, particularly in the price of assets. This fast inflation is followed by a quick decrease in value or a contraction, which is sometimes referred to as a "crash" or a "bubble burst". Bubbles are generally a characteristic of a scam that is trying to defraud wealthy investors.
- Exchange: An exchange is a service that individuals and companies can use to trade one cryptocurrency for other cryptocurrencies or fiat to a cryptocurrency.
- Mixers: As we already know, the anonymity of a user is one of the highly preferred features of cryptocurrency, and mixers are used to further strengthen it. Cryptocurrency is deposited into a smart contract designed to execute a mixing transaction from a single address. Users can withdraw previously deposited tokens from another address after a predetermined period of time. Mixers have their own protocol for performing the mixing action, which makes it difficult to track the coins when they are put into a mixer. This is exploited by scammers to escape with the coins that they managed to scam from investors.

Now that we understand how blockchain and cryptocurrencies work, let us look at different types of scams that have startled the financial sector by stealing billions of dollars.

- Ponzi schemes: A Ponzi scheme is a fraudulent investment scheme in which an operator pays returns on investments from capital derived from new investors rather than from legitimate investment profits. Ponzi schemes generally fall apart when there is not enough new capital to pay the ever-growing pool of existing investors. Cryptocurrency Ponzi schemes are very common and have resulted in huge losses. OneCoin, BitClub CoinUp, MMM Bitcoin, and PlusToken are popular Ponzi schemes that defrauded investors out of billions of dollars worth of cryptocurrency [17].
- Pump and dump schemes: Pump-and-dump schemes involve accumulating commodities over time, inflating their prices by spreading misinformation (pumping), then selling them at higher prices to unsuspecting buyers (dumping). Due to artificial inflation, the price usually drops, leaving buyers who bought based on false information at a loss. In 2018, pump and dump schemes accumulated about $825 millions from naive investors [7].
- Initial Coin Offering (ICO) Scams: As already mentioned, ICOs can be launched by anyone to raise investment for their project. Scammers take advantage of ICOs to launch coins, mine coins, or create a service. In the end, they cash out the investor's money and leave the coins they sold with no value. ICO scams can be understood with the help of critically reading the white papers and checking for misleading or copied contents [15].
- High-Yield Investment Programs (HYIP): high-yield investment programs (HYIPs) are Ponzi schemes that promise high returns on investments in short periods of time. These programs have cheated investors out of millions of dollars. On 23 July 2013, the Securities and Exchange Commission (SEC) charged a Bitcoin-based HYIP scammer who offered a 7% daily interest rate to investors and cheated them out of 700,000 BTC, valued at over 1 billion dollars today. [18].
- Money laundering: Money laundering is the illegal process of making "dirty" money appear legitimate instead of ill-gotten. Criminals use a wide variety of money-laundering techniques to make illegally obtained funds appear clean. Online banking and cryptocurrencies have made it easier for criminals to transfer and withdraw money without detection. The prevention of money laundering has become an international effort and now includes terrorist funding among its targets. The financial industry also has its own set of strict anti-money laundering (AML) measures in place [19].
- Crypto hacking: Crypto hacking refers to the hacking of user wallets to spend or steal cryptocurrency from these accounts. The scammers usually use ransomware

or phishing techniques to steal the private keys of the users and hack into their accounts [20].

- Market manipulation: Market manipulation is the deliberate attempt to artificially influence or interfere with asset prices. Scammers manipulate the market in multiple ways:
  - Spoofing: Creating illusions to cheat investors. Scammers use dummy accounts and bots to place large trades, which are canceled before they are filled, giving other investors the impression that demand is either increasing or decreasing.
  - Front running: The practice of making trades based on knowledge of future transactions. Miners and node operators have insights into upcoming trades, which can be used for personal gains.
  - Churning: Excessive trading by a broker in a client's crypto account to generate additional commissions. Asset management firms can receive fees for managing crypto holdings. Therefore, nefarious brokers could abuse a commission-based payment structure to profit off of unaware clients, which could also leave the clients with tax liabilities.
- Giveaway scams: A giveaway scam is very common nowadays. Scammers use social media pages such as YouTube [21] and Twitter to attract investors by saying that a new project or scam is highly functional. They point to websites with fake information and give wallet addresses of scammers asking investors to send money for high returns.

Over the decade, several scams have stolen billions of dollars and caused severe harm to the global economy. Research works have aimed to detect these scams using multiple approaches and have succeeded in identifying them. Understanding the architecture and functioning of blockchain technology, cryptocurrencies, scams, and detection techniques is crucial to analyze these areas. Similarly, it is very important to know the current trends and happenings on them to produce valid results on detection techniques that align with the current day scenario. Keeping up to date with scams, currency values, market capital, and the rankings of cryptocurrencies can help us understand the seriousness of the issue and thus to evaluate detection models meticulously. Two types of data that can help us achieve this are:

- News articles, blogs, and reports published by trusted resources.
- Official websites such as blockchain.com, coinmarketcap.com, and etherscan.io show real-time transactions and values of cryptocurrencies equivalent to fiat currencies.

News articles published by financial giants such as The Wall Street Journal, Bloomberg Businessweek, Forbes, and Financial Times report detailed information on scams, their technique, the value of money lost in the scam, the action taken against the scammers, and the status of the victims and their funds. For example, [22] published by The Wall Street Journal and [23] by Forbes unveil scams caused by a Ponzi Scheme and a Pig Butchering activity (targeted scamming of rich individuals by scammers) respectively. The former has managed to lure more than 100,000 investors with false promises. These articles also talk about general market trends analyzing various aspects of the cryptocurrency industry, such as [24], which provides insights into the effects of inflation, market sliding, and the crippling of the economy on cryptocurrencies and how the value of cryptocurrencies has dropped to 2/3rd of its value in June 2022. Similarly, [25] by Financial Times summarizes how the lack of regulations leads to scams in crypto. These articles also categorize and rank cryptocurrencies, projects, exchanges, and crypto-platforms [11] that can be useful for future predictions.

Other than these news articles and reports, transactions on the public ledger of blockchain are available in websites including blockchain.com [26], which can be used as a source to validate legitimate transactions. Etherscan.io [27] also lists transactions in Ethereum and its market capital. Exchanges such as Binance [28] and Coinbase [29] list values of different coins equivalent to fiat currencies and aid in exchanging coins to fiat currencies and vice versa. coinmarketcap.com [30] shows the market value of multiple

coins at any point of the day and helps investors to decide the best options to invest in. In general, investopedia.com provides definitions, explanations, and examples of various cryptocurrency-related concepts that help investors and researchers to understand the technology better.

Governments, big corporations, officials, and investment-advising agencies are working towards building regulations and have put forward measures such as anti-money laundering (AML) and know your customer (KYC) to limit these scams. We will be looking at works that have applied computing solutions to detect these scams along with similar surveys that have aimed to compile data that is available in the next section.

3. Related Work

Blockchain technology and cryptocurrencies have attracted research attention over the past decade. In an effort to collect and compile the research works, we have categorized them based on their purpose and approach to the problems. The categories we have considered are given in Table 1.

Table 1. Categories of research works and peer-reviewed articles.

Category	References
Textbooks, architectures, and processes	[1,6,7,9,12,14]
Existing surveys, literature reviews, and analysis publications	[5,31–40]
Detection techniques on scams in cryptocurrencies using machine learning algorithms	[18,19,41–65]
Other type of approaches to solve scams	[15,66–68]

To understand the fundamental concepts and workings of blockchain technology and cryptocurrencies, we have used textbooks, glossaries, and peer-reviewed articles. The first whitepaper published by Satoshi Nakamoto in 2008 introduced blockchain and Bitcoin. This paper provides detailed information on the working of the technology and its concepts. The Federal Trade Commission (FTC) released a glossary [6] in the Annual National Seminar in 2018 that defines all of the important cryptocurrency-related terms. The authors of [7,9,12] explain the working of a blockchain, the consensus mechanism, and how transactions are carried out for different services. Iansiti and Lakhani in [7] compared the growth of blockchain technology to the invention of emails and have provided insights to support the fact that cryptocurrencies will be the currencies of the future. In [12], Yuan and Wang provided a detailed explanation of the different layers in the architecture of the blockchain and its types, which help in identifying threats for different services.

In the literature, several works have already aimed to study, compare, and compile existing research on blockchains and cryptocurrencies. There are surveys, literature reviews, and conceptual papers that have analyzed different areas of this technology and the scams that devalue them. Few publications look into all the cryptocurrencies such as Bitcoin and Ethereum, while others focus on one particular coin. Similarly, they also look into different types of scams and produce an analysis of each scam, or they choose any scam such as Ponzi schemes or money laundering.

Surveys that analyze all cryptocurrencies, the scams that occur in them, and the defensive mechanisms are given in [31,37,38]. These surveys approach the technology and scams in different ways. In [31], Phan et al. studied scams and common issues by analyzing tweets on the blockchain. For the period of 8th November to 31st December 2018, over 2 million tweets mentioning 'blockchain' as a keyword were collected using a tweet listener created using Apache Flume. Observations of their analysis concluded that 69% of the tweets on the blockchain were negative. A systematic literature review by Badawi and Jourdan [37] identified several peer-reviewed articles on scams and defensive mechanisms. In this paper, a variety of information and statistics on different groups of peer-reviewed articles were provided. UmaMaheshwaran et al. in [38] conducted a

survey on understanding the types of mechanisms used and their effectiveness in detecting scams. Survey questions were posted to a group of 75 people who traded cryptocurrencies and had blockchain knowledge. The observations of this survey stated that over 35% of the respondents believed that machine learning methods are useful to detect fraud in cryptocurrencies.

The importance of regulations, international standards, and authorization over cryptocurrencies are stated by [32,34]. Teichmann and Falker in [32] studied how cryptocurrencies are used for financial crimes and proposed a more effective international standard for regulation. This study talks about the mindsets of criminals, experts, and authorities and how they can help in proposing regulations. In [34], the problem of money laundering is exposed, and the open doors in blockchain technology are discussed by Dupuis and Gleason. This work also talks about the importance of regulations for exchanging cryptocurrencies.

Surveys such as [35,36,40] look into cryptojacking, exchange scams, and Ponzi Schemes, respectively. Cryptojacking is the practice of unauthorized use of computation resources of individuals or organizations to mine cryptocurrencies. Jayasinghe and Poravi, in [35], aimed to look at cryptojacking instances on the cloud infrastructure and discussed various platforms as well as mechanisms used to hack into cloud servers. In a nutshell, this paper introduced cryptojacking, analyzed the attack on cloud resources, reviewed the existing literature, talked about research gaps, and suggested a detection system using behavioral analysis for the future. In [36], Xia et al. exposed scams in exchanges and fake exchanges that operated to steal cryptocurrencies. The authors have identified 1595 exchange scams, of which over 60% of the scams are unknown, and 300+ fake exchange apps, which are even available in legitimate play stores such as google play. This work used a clustering approach to group these scams and fake apps into families and ended up with 94 scam families and 30 fake app families. As per this paper, the financial loss due to the exchange scams at the time of 2018 was evaluated at 520K USD.

Xia et al. in [39] reported that the number of scams and losses increased drastically during the COVID-19 period. This research compiled different types of scams that occurred in cryptocurrencies. During the world crisis, scammers took advantage of and unleashed several crypto crimes using the name of COVID-19. There were 195 scams reported, including 91 token scams (ICOs), 9 blackmail scams, 14 malware scams, 9 Ponzi schemes, and 53 donation scams that used COVID-19 as bait. The authors studied these scams, analyzed their characteristics, and explored the tricks and social engineering activities the scammers used. While other papers focus on scams and detection techniques, [5] by Adhami et al. look into the brighter side of cryptocurrencies and produce a survey on the success of startups that use cryptocurrencies to raise investments. The authors proposed a hypothesis that marks the success of an ICO based on the availability of future outlook, whitepapers, and the source code of the project to the investors. Additionally, other characteristics such as presale, bonus schemes, and advantages over services such as marketplaces and coupons increase the success of an ICO.

Detection techniques use multiple approaches to spot scams in cryptocurrencies based on various aspects. While the next section explains each technique, the datasets used and the features extracted, in this section, let us look at some common observations in these techniques that helped us to identify these publications. Generally, these algorithms look into one type of scam and try to train a model to detect the scam. For example, [19] proposed a model to identify money laundering, while [59] looked into pump and dumps. Table 2 provides a list of scams and references that are studied in this survey. Another common observation is that these techniques also look into one type of cryptocurrency such as Bitcoin to identify malicious activities in accounts and detect transactions as valid or invalid. Bitcoin and Ethereum are the most commonly studied cryptocurrencies in the literature.

Table 2. Types of scams and their references.

Category	References
Ponzi Schemes	[42,48–50,58,63,65]
Money Laundering	[19,54,69–71]
Pump and Dump	[43,59–61]
Cryptojacking	[46,51–53]
Phishing	[62,68,72,73]
Fake Wallets/Accounts	[55,57,64,74]
Exchange Scams	[36]
HYIP	[18,75]
Ransomware	[56]
DDoS attack	[45]

Compared with previous surveys, in this work we have studied scams and solutions in cryptocurrencies in more detail and categorized existing works on each scam and the machine learning methods adapted to address each type of scam. We have also discussed the type of features, transaction data, and outcomes of these models, which are not presented in previous surveys.

Table 3 provides the list of cryptocurrencies and references that examined the currencies, respectively. In this section, we have categorized and explained the resources we have considered for our survey.

With a background of concepts and a review of literature, the next section discusses the solutions proposed to address the scams and surveys their performances.

Table 3. Types of cryptocurrencies and their references.

Category	References
Bitcoin	[18,19,41,42,44,47,54,57,59,75]
Ethereum	[48–50,55,58,62–64,74]
Cryptocurrencies in general	[43,46,52,53,56,60,61]

4. Performance Analysis of Detection Models

As the use of digital wallets and cryptocurrencies increased, the number of scams and felonious activities hindering their growth also increased. According to a report by CNBC [76], scammers have cheated more than $14 billion in 2021, with a 516% raise from 2020. Rug pulls, Ponzi schemes, and pyramid schemes have contributed largely to this loss. This report also said that crypto-related crimes were at an all time high during the time, which was when the scams that took advantage of COVID 19 situations were at a peak. Scams and fraud have always existed in society. Experts say that these scams have evolved with technology, but their motive to defraud innocent people or investors for their own gain has not changed. Governments, corporations, investment advising companies, and authorities are always on the hunt to identify these scams for the wellness of the economy and people by observing these characteristics. Research has been conducted to develop computational models that can detect these scams as well as prevent them.

In this section, we have categorized the models based on the type of scam they try to detect and analyzed their performance metrics, feature extraction methods, and datasets used. This effort aims to provide a compilation of existing scam detection models that perform optimally under a variety of conditions. As a part of our evaluation of these models, we considered performance metrics such as precision, recall, and F1 score. A model's precision is how accurate it is in predicting one particular type of event. Recall

is essentially a measure of how often a model can correctly identify a category based on the data it receives. The harmonic mean of precision and recall is widely used to compare different models and algorithms. Our study has also addressed these models and classified them based on the types of cryptocurrencies in which they have attempted to detect scams.

We have categorized each machine learning model into the type of scam it aims to detect. The results of their efficiency were obtained from the results discussed in each paper. The primary reasons to compare the results from different works, which are executed on different datasets, are as follows: the datasets used by these works consisted of scam-related transactions and valid transactions of the same type of cryptocurrencies or the same type of scam. The features used in these models are similar, and the algorithms used have the same type of approach. These models are intended to detect cryptocurrency scams, and the success rate of each of them indicates how accurate and efficient they are at doing so.

4.1. Ponzi Schemes

As mentioned in the previous sections, Ponzi schemes are one of the most common types of scams that have embezzled millions of dollars over the decade. Research studies and detection models have identified Ponzi schemes largely in both Bitcoin and Ethereum. In order to detect these scams, machine learning models have differentiated two types of features and have also tried to compare their impact on identifying scams. In Ethereum, smart contracts have examined datasets, then features have been separated into two categories: code and account [48–50]. In code features, the bytecode of the smart contracts is analyzed to identify patterns or commonly occurring pieces of code that can be used to differentiate a Ponzi scheme and a non-Ponzi scheme smart contract. A performance metric analysis of code features of multiple models surveyed is shown in Figure 1. Account features look into behavioral activities such as balance, transaction frequencies, ETH in, and ETH out, for detecting fraudulent activities. Figure 2 shows the analysis of account features, and Figure 3 provides the analysis of both features combined.

In [50], Chen et al. collected real-world data that can be reused for future research and proposed a detection technique to identify Ponzi schemes. Two types of datasets were collected manually by checking open-source smart contracts on the Ethereum platform. The first dataset used to build a classification model consisted of all of the labels and features of the 3780 open-source contracts. Another dataset contained code features of all of the smart contracts (including open-source contracts and hidden-source contracts), which were used to approximate the number of smart Ponzi schemes running on the Ethereum platform. This paper used multiple machine-learning algorithms to build models and compared their performances for three categories of features. The three categories were using account and code features separately and combined them to predict the illicit smart contract. Chen et al. authored [48] as preliminary research to construct the dataset and build a detection model using XGBoost. In a similar fashion, Jung et al., in [49], developed detection models by analyzing the same three categories of features. The authors focused on identifying Ponzi schemes right from the day they are added. They compared the 0-day performance to the 248-day performance on the smart contracts by using the level of features available using the J48 decision tree, Random Forest, and Stochastic Gradient Descent algorithms to detect Ponzi schemes.

In [42], Bartoletti et al. created a dataset of features of real-world Ponzi schemes, which they constructed by analyzing the Bitcoin blockchain and the transactions used to perform the scams. They approached the problem as a binary classification problem and experimented with three classification models to identify the best performance. In this effort, the authors achieved an accuracy of detecting 31 out of 32 Ponzi schemes in their dataset. Hu et al., in [58], proposed SCSGuard, a novel deep-learning scam-detection framework that analyzed code features of smart contracts to detect any kind of scam in them. The framework was based on n-gram features and attention neural networks of the bytecode of the smart contracts to detect scams. The model achieved an accuracy of 92.2% to detect Ponzi schemes and an accuracy of 94.7% to detect Honey pots.

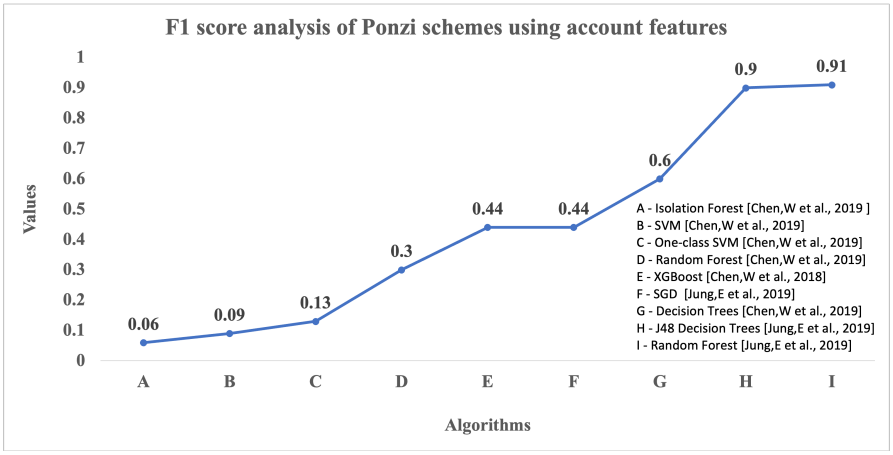

Figure 1. F1 score comparison of Ponzi schemes with account features.

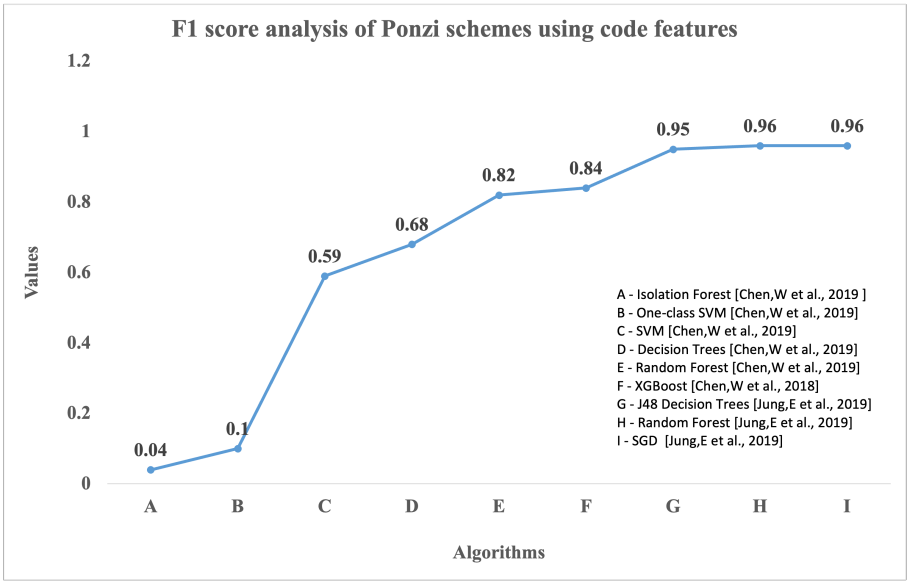

Figure 2. F1 score comparison of Ponzi schemes with code features.

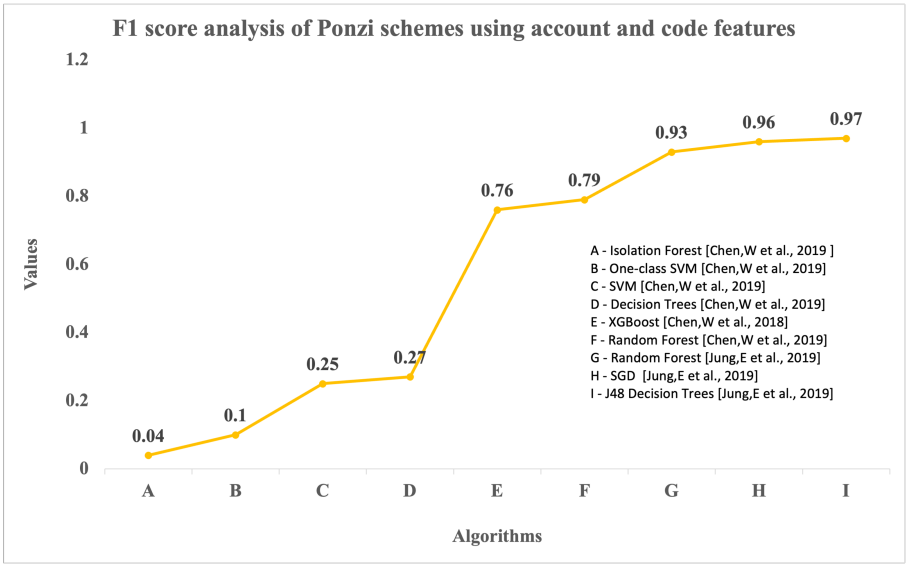

Figure 3. F1 score comparison of Ponzi schemes with account and code features.

4.2. Money Laundering

Money laundering activities have caused serious losses in cryptocurrencies and have attracted research to study their characteristics and build detection models. In general, models proposed to detect money laundering try to classify transactions into illicit and valid classes and primarily use account features such as account balance, money in, and money out for training. In [19,54], Alarab et al. explore the Elliptic dataset, which is derived from the Bitcoin blockchain and represents transactions in the form of a directed graph network of nodes representing transactions from sources to destinations. The graph structure of the dataset motivates them to use neural networks to develop a detection model. The proposed model [19] combines graph convolutional networks with linear layers and multilayer perceptron (MLP) to provide 97.4% accuracy in identifying illicit transactions in the Elliptic dataset. In [54], a comparison of supervised learning models—Random Forest, Extra Trees, Bagging, AdaBoost, Gradient Boosting, and k- Nearest Neighbors—are performed, and an ensemble learning model combining Random Forest, Extra Trees, and Bagging is proposed to detect money laundering activities.

A comparison of the performance metrics of all the models identified under the money laundering scams is displayed Figure 4. Lorentz et al., in [69], explained the disadvantage of supervised learning models when labels are scarce in the elliptic dataset. With a realistic label condition, they proved that active learning methods detected illicit transactions with high accuracy with 5% of labels used by supervised learning. The authors also proved that unsupervised learning models have poor performance in a similar environment. Badawi and Al-Haija, in [70], also used an elliptic dataset to build machine learning models to detect money laundering activities. This paper compared the performance of the neural network and decision tree models in detecting felonious activities. For providing multi-class classifications using a probability distribution function that assigns every output class a probability value, the authors have used Softmax classifiers and showed that shallow neural networks and decision trees achieve classification accuracy capped at 89.9% and 93.4%, respectively. Baek et al., in [71], used an unsupervised learning expectation-maximization algorithm to cluster the data and extract features of Ethereum transactions in the real world blockchain ledgers. With the features engineered from the unsupervised learning, anomaly detection is performed using the Random Forest algorithm to identify discernible transactions.

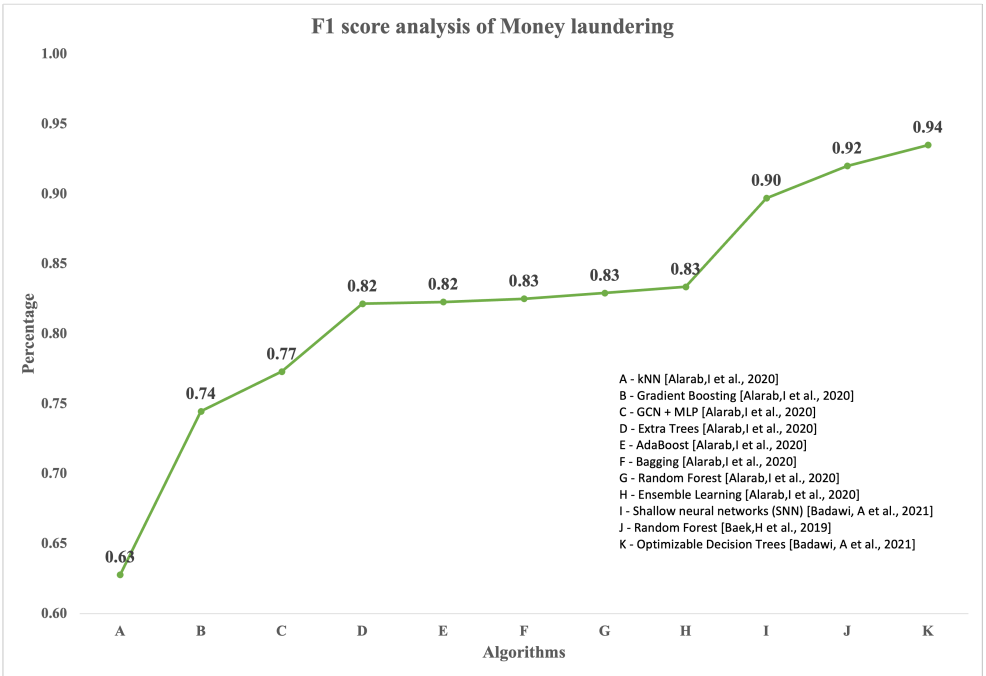

Figure 4. F1 score comparison of money laundering.

4.3. Pump and Dump

Pump and dump scams have now become common in Bitcoin and Ethereum blockchains. The Mt. Gox Exchange scam, which was a notorious scam in which millions of dollars was embezzled, was studied by Chen et al. in [61]. This work discusses the importance of bringing regulations to the crypto market. The authors proposed an improved Apriori algorithm to detect cryptocurrency pump and dump schemes. Observations concluded that the Mt. Gox exchange had fake trading volume. The model explored transactions and their relations to user ids to identify patterns in transaction records such as buying or selling by the users at the same time and the number of Bitcoins bought or sold and identified the pump and dump phases of the scam.

4.4. Phishing

Machine learning models have exploited the network features mainly to identify phishing scams. As we know that phishing scams start from fake links on web pages and social media posts to a scammers address, these models target the network features. In [62], Yuan et al. created a network of transactions as their dataset and proposed a model that uses the node2vec network embedding method to extract features from the transactions and uses one-class SVM (support vector machine) to classify the user accounts into phishing accounts and other accounts. Similarly, in [68], J. Wu et al. uses trans2vec network embedding to extract features and uses Logistic Regression, Naive Bayes, Isolation Forest, and One-Class SVM algorithms to build models and compare their results in detecting phishing scams. Figure 5 shows the comparison of the F1 score comparison of these models. Wen et al., in [72], extracts both the network and account features of transactions to propose a phishing detection framework and an adversarial attack framework and define metrics to show that the model is optimal to detect phishing activities in Ethereum. Transaction data publicly available in etherscan.io and other websites are widely used to form datasets to identify phishing addresses and transactions related to them.

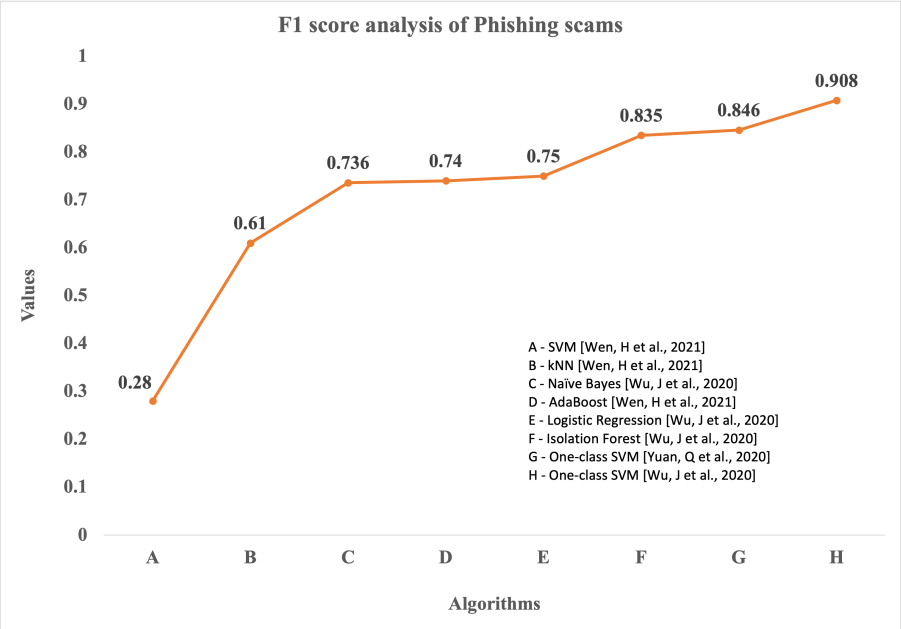

Figure 5. F1 score comparison of phishing scams.

4.5. Fake Wallets and Accounts

Fake user accounts and wallets are considered a problem for the blockchain by several researchers as they hinder the working of the technology and makes it vulnerable to scams and other criminal activities. To identify fake accounts, models have widely used the account features and used machine learning algorithms to detect the fake accounts.

Farrugia et al., in [55], used the XGBoost classifier to detect fraudulent accounts based on the transaction history of these accounts in Ethereum and achieved an accuracy of 96.3%. The authors also provided insights into important features that can help build a highly accurate detection model and create a compiled dataset for future research. In [57], Shayegan et al. proposed a collective anomaly approach to identify fake users in Bitcoins. This approach used the trimmed_Kmeans algorithm for data clustering and successfully identified 14 users who owned multiple accounts that committed fraud in 9 different cases. The authors have also discussed the importance of reducing the processing power and computational time in the models and proved that the proposed model has detected a very large number of fake users even with a reduced number of records and features from the state-of-art models. Ostapowicz and Zbikowski in [74] apply supervised learning techniques to detect fraudulent accounts on Ethereum. They also compared the working capabilities of Random Forest, the support vector machine, and XGBoost classifiers on a dataset of more than 300 thousand accounts. This work also discussed the sensitivity analysis of these models by examining their feature dependency and system performance. Kumar et al., in [64], detect suspicious accounts on the Ethereum blockchain by analyzing the two types of accounts–Externally Owned Accounts (EOA) and smart contract accounts. After preprocessing the data for both types of analysis, the authors use kNN, Decision Tree, Random Forest, and XGBoost classifiers using Python's Scikit-learn library. Figure 6 shows the comparison of the accuracy comparison of these models.

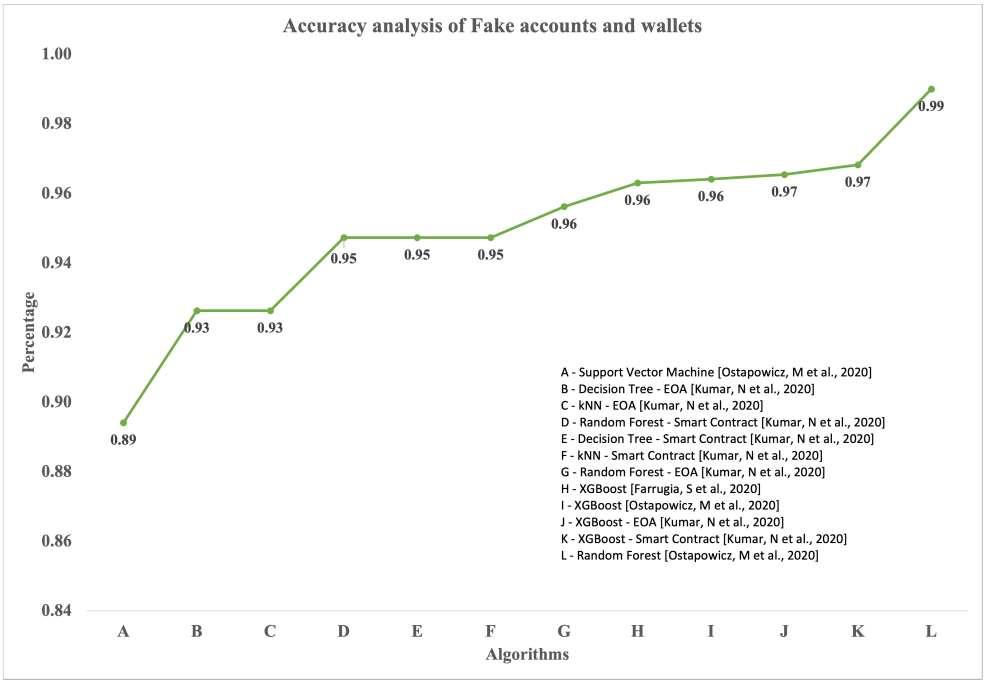

Figure 6. Accuracy comparison of fake wallets and accounts.

4.6. Cryptojacking

Cryptojacking refers to mining attacks that are common nowadays in which cryptocurrencies are stolen directly from users' CPU or computational power without their knowledge. This attack leads to several losses, and models have been proposed to identify them. In [53], Zimba et al. demonstrate that integrating semi-supervised learning with complex network theory modeling effectively detects crypto-mining activities. The proposed approach uses network characteristic features of the dataset, creates clusters using the Shared Nearest Neighbor algorithm, and uses the KNN classifier to train a model to detect crypto-mining activities. In short, the semi-supervised learning approach uses the unsupervised learning method to extract features from the unlabeled dataset, and the supervised model classifies this data instances of crypto mining using complex network

characteristics features. OUTGUARD is an automated cryptojacking detection system proposed by Kharraz et al. in [46] that uses seven distinctive features with an SVM classification model. The authors created a dataset using real-world data and achieved a 97.9% true positive rate and a 1.1% false positive rate. Similarly, CapJack, proposed by Ning et al. in [52], is another in-browser malicious cryptocurrency mining detecting model that uses neural networks to detect illegal crypto mining. This model has high accuracy—from 87% to 99% within a window of 11 s when executed on real-time browser data.

From our analysis, it is evident that scams and scammers use different approaches and exploit the varied characteristics of blockchain technology to fraud investors. In this section, we discussed different scam types and the models that attempted to identify the patterns and characteristics of these scams to successfully detect them in real-world datasets. In addition, it is also worth mentioning that most of the machine-learning models have focused on Bitcoin and Ethereum. Several other observations that are worth mentioning are discussed in the following section of this paper. In this section, the models that perform best under multiple categories are also highlighted.

5. Results and Observation

From the previous section, a review of existing scams, their characteristics, the models used to approach each type of scam, and their performances have been attained. By categorizing the scams, several observations and conclusions are obtained from these models, which will be discussed in this section. In general, we can see that research works have primarily focused on Bitcoin and Ethereum cryptocurrencies, which constitute more than 45% of the capital value of the cryptocurrency market. As already mentioned, the scam rates have drastically increased in recent years. The COVID 19 era sparked a golden age of crypto scams [39]. It was during this time that several scam techniques such as wash trading, giveaways, emergency scams, and referrals saw peaks. From 2008 to 2013, over 500 Ponzi schemes scammed over $50 billion , which is exactly when the very first cryptocurrency Bitcoin was introduced and started growing. Over the decade, detection models using machine learning techniques have been developed to detect these scams and have achieved optimal results.

As we saw that Ponzi schemes contribute a high percentage of scams, machine learning models have achieved high efficiencies in detecting them. From the performance analysis conducted, we can see that to detect Ponzi schemes, these models have categorized the features of the dataset into account and code subsets. From [48–50], it is evident that code features and a combination of both the features perform with high efficiency. Random Forest, J48 Decision Trees, and Stochastic Gradient Descent algorithms have achieved very high F1 scores of 93%, 97%, and 96%, respectively, while using a combination of both the features. The XGBoost algorithm has performed fairly better when compared with the other algorithms mentioned in the performance analysis of the Ponzi schemes. The deep learning application of neural networks has also demonstrated very good performance, producing 96.3% precision, 97.8% recall, and an F1 score of 97.1%.

Money laundering has always been a problem for financial stability and has created issues with cryptocurrencies. As mentioned in the analysis section, the Elliptic dataset has been commonly used to develop a detection model. Binary classification of valid and illicit transactions has been applied to detect money laundering. Clustering the data using an expectation-maximization algorithm to extract features to detect laundering with Random Forest by Baek et al., [71] has shown highly efficient performance with a F1 score of 92%. Badawi and Al-Haija's comparison of neural networks and decision trees has also performed well with F1 scores of 89.7% and 93.5%, respectively, in identifying money laundering [70]. Additionally, algorithms such as Extra Trees, Bagging, Ada Boost, and the ensemble method in [54] have done well, with F1 scores over 80%.

Generally, network features are used to detect phishing, while account features are used to detect fake accounts. One class SVM algorithm used by both [62,68] has performed well, with F1 scores of 84.6% and 90.8%, respectively, to determine phishing. Both of

these papers use network embedding methods to extract features and have performed better than [72], which used mining techniques. In the case of fake wallets, all of the surveyed models have shown excellent performances, with an accuracy of over 89.3%. In [74], the Random Forest algorithm used on account features of a dataset with more than 300 thousand accounts achieved 99.51% accuracy, which constitutes very high efficiency when compared to any other model in any category.

Regarding cryptojacking or illegal mining, performance analysis has identified reasonably performing models. Similarly, in the case of other scams such as HYIP [18,75] and Pump and dumps [61] we have identified research works that have attempted to identify the characteristics and developed techniques that detect the fraudulent transactions. The performance analysis section helped us to come to these conclusions, which were discussed in this section. Features, datasets, and important characteristics were thus listed successfully.

Depending on the type of scam, features were selected by each model to detect them. Some common features that may be useful in identifying scams include:

- Transaction amount: Large transactions or transactions with unusual amounts may indicate a scam.
- Destination address: Scammers often use addresses that are known to be associated with scams, so checking the destination address against a blacklist of known scam addresses can be useful.
- Sender address: The identity of the sender may also provide clues about the nature of the transaction. For example, if the sender's address is associated with a known scammer, this may indicate a scam.
- Time of transaction: Scammers often act quickly, so transactions that occur over a short period of time are more likely to be scams.
- Contract code: The code associated with the transaction can provide additional information about its purpose. For example, if the contract code is associated with a known scam, this may indicate a scam.
- Network behavior: The behavior of the transaction on the network, such as the number of inputs and outputs, can also provide clues about its nature.
- Previous transactions: The history of the addresses involved in the transaction, including the amount and number of previous transactions, can provide additional information about the nature of the transaction.

These features are commonly divided into categories such as code features, network features, and transaction features and are used to detect scams in cryptocurrencies.

We believe that this survey will help researchers understand the existing scams, detection models, and techniques available in cryptocurrency technology and provide insights and ideas with which to work further on them. In the next section, we give our concluding comments and suggestions for further research in this area.

6. Conclusions

In this survey, we have understood the key concepts of blockchain technology and cryptocurrencies, studied the characteristics of scams in them, and seen how machine learning models exploit these characteristics to detect scams. With this review, we can clearly see that the techniques used to detect these frauds have also evolved and have performed very efficiently. Our performance analysis has identified the best performing models, datasets, and features for various scam types. We have used measures such as accuracy, precision, recall, and F1 score to compare these models. Beyond these metrics, a machine learning model's performance can be validated by other attributes such as time complexity, the number of nodes used, the number of features used, the number of epochs, computational power used, and so on. Beyond machine learning, there are detection models or techniques that identify scam activities by investigating fake websites, social media posts, giveaway links, phishing links, and forwarded messages. These techniques can also be examined and used for further research or surveys.

Author Contributions: Conceptualization, L.P.K.; methodology, L.P.K.; investigation, L.P.K.; data curation, L.P.K.; writing—original draft preparation, L.P.K.; writing—review and editing, I.V., S.R. and S.A.; visualization, L.P.K.; supervision, I.V., S.R. and S.A.; project administration, I.V., S.R. and S.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 21 December 2022).
2. Statista.com. Cryptocurrency Statistics from Statista. Available online: https://www.statista.com/topics/4495/cryptocurrencies/ (accessed on 21 December 2022).
3. Coinmarketcap.com. Rankings, Values and Statistics from Coinmarketcap.com. Available online: Coinmarketcap.com (accessed on 21 December 2022).
4. Commission, F.T. Data Spotlight, Reports Show Scammers Cashing in on Crypto Craze. 2022. Available online: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze (accessed on 21 December 2022).
5. Adhami, S.; Giudici, G.; Martinazzi, S. Why do businesses go crypto? An empirical analysis of initial coin offerings. *J. Econ. Bus.* **2018**, *100*, 64–75. [CrossRef]
6. United States Sentencing Commission. *Bitcoin Glossary: 2018 Annual National Seminar*; United States Sentencing Commission: Washington, DC, USA, 2018.
7. Iansiti, M.; Lakhani, K.R. The truth about blockchain. *Harv. Bus. Rev.* **2017**, *95*, 118–127.
8. Tharani, J.S.; Charles, E.Y.A.; Hóu, Z.; Palaniswami, M.; Muthukkumarasamy, V. Graph Based Visualisation Techniques for Analysis of Blockchain Transactions. In Proceedings of the 2021 IEEE 46th Conference on Local Computer Networks (LCN), Edmonton, AB, Canada, 4–7 October 2021; pp. 427–430. [CrossRef]
9. Islam, M.N.; Hossen, M.G.S.; Baidya, S.P.; Emon, M.A.U.; Hossain, M.S. A Framework for Tracing the Real Identity of a Bitcoin Scammer. In Proceedings of the 2021 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2), Rajshahi, Bangladesh, 26–27 December 2021; pp. 1–4. [CrossRef]
10. coindesk.com. How Crypto Could Spearhead Retail Payments in 2022. Available online: https://www.coindesk.com/layer2/paymentsweek/2022/04/29/how-crypto-could-spearhead-retail-payments-in-2022/ (accessed on 21 December 2022).
11. Forbes. Top 10 Cryptocurrencies of 2022. Available online: https://www.forbes.com/advisor/investing/cryptocurrency/top-10-cryptocurrencies/ (accessed on 21 December 2022).
12. Yuan, Y.; Wang, F.Y. Blockchain and Cryptocurrencies: Model, Techniques, and Applications. *IEEE Trans. Syst. Man Cybern. Syst.* **2018**, *48*, 1421–1428. [CrossRef]
13. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.Y. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 2266–2277. [CrossRef]
14. Investopedia. Initial Coin Offering (ICO): Coin Launch Defined, with Examples. Available online: https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp#:~:text=An-initial-coin-offering-(ICO)-is-the-cryptocurrency-industry's-equivalent,a-way-to-raise-funds (accessed on 21 December 2022).
15. Morin, A.; Vasek, M.; Moore, T. Detecting Text Reuse in Cryptocurrency Whitepapers. In Proceedings of the 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Sydney, Australia, 3–6 May 2021; pp. 1–5. [CrossRef]
16. Forbes. Cryptocurrency Glossary of Terms and Acronyms. Available online: https://www.forbes.com/advisor/investing/cryptocurrency/crypto-glossary/ (accessed on 21 December 2022).
17. Mukherjee, S.; Larkin, C. Cryptocurrency Ponzi schemes. In *Understanding Cryptocurrency Fraud*; Corbet, S., Ed.; De Gruyter: Berlin, Germany; Boston, MA, USA, 2022; pp. 111–120. [CrossRef]
18. Toyoda, K.; Mathiopoulos, P.T.; Ohtsuki, T. A novel methodology for hyip operators' Bitcoin addresses identification. *IEEE Access* **2019**, *7*, 74835–74848. [CrossRef]
19. Alarab, I.; Prakoonwit, S.; Nacer, M.I. Competence of graph convolutional networks for anti-money laundering in Bitcoin blockchain. In Proceedings of the 2020 5th International Conference on Machine Learning Technologies, Beijing, China, 19–21 June 2020; pp. 23–27.
20. Insider, B. 5 Crypto Scams to Know before You Start Trading Coins, Business Insider. Available online: https://www.businessinsider.com/personal-finance/crypto-scams (accessed on 21 December 2022).
21. Vakilinia, I. Cryptocurrency Giveaway Scam with YouTube Live Stream. In Proceedings of the 2022 IEEE 13th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 26–29 October 2022; pp. 0195–0200.

22. The Wall Street Journal. SEC Charges Trade Coin Club Founder, Promoters in $295 Million Bitcoin Fraud. Available online: https://www.wsj.com/articles/sec-charges-trade-coin-club-founder-promoters-in-295-million-Bitcoin-fraud-11667598959?mod=business_minor_pos16 (accessed on 21 December 2022).
23. Forbes. How One Man Lost 1 Million Dollar to a Crypto 'Super Scam' Called Pig Butchering. Available online: https://www.forbes.com/sites/cyrusfarivar/2022/09/09/pig-butchering-crypto-super-scam/?sh=3930764bec8e (accessed on 21 December 2022).
24. The Wall Street Journal. The Crypto Party Is Over. Available online: https://www.wsj.com/articles/the-crypto-party-is-over-11655524807 (accessed on 21 December 2022).
25. Times, F. The Lawless World of Crypto Scams. Available online: https://www.ft.com/content/5987649e-9345-4eae-a4b8-9bfb0142a2ab (accessed on 21 December 2022).
26. Blockchain. Official Blockchain Website. Available online: www.blockchain.com (accessed on 21 December 2022).
27. Etherscan.io. Ethereum Website. Available online: www.etherscan.io (accessed on 21 December 2022).
28. Binance. Exchange Platform: Binance. Available online: https://www.binance.com/en (accessed on 21 December 2022).
29. Coinbase. Exchange Platform: Coinbase. Available online: https://www.coinbase.com/ (accessed on 21 December 2022).
30. Coinmarketcap. Coinmarketcap.com. Available online: https://www.coinmarketcap.com/ (accessed on 21 December 2022).
31. Phan, L.; Li, S.; Mentzer, K. Blockchain technology and the current discussion on fraud. *Comput. Inf. Syst. J.* **2019**, *20*, 8–20.
32. Teichmann, F.M.J.; Falker, M.C. Cryptocurrencies and financial crime: Solutions from Liechtenstein. *J. Money Laund. Control* **2021**, *24*, 775–788. [CrossRef]
33. Desmond, D.B.; Lacey, D.; Salmon, P. Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review. *J. Money Laund. Control* **2019**, *22*, 480–497. [CrossRef]
34. Dupuis, D.; Gleason, K. Money laundering with cryptocurrency: Open doors and the regulatory dialectic. *J. Financ. Crime* **2020**, *28*, 60–74. [CrossRef]
35. Jayasinghe, K.; Poravi, G. A survey of attack instances of cryptojacking targeting cloud infrastructure. In Proceedings of the 2020 2nd Asia Pacific Information Technology Conference, Bali Island, Indonesia, 17–19 January 2020; pp. 100–107.
36. Xia, P.; Wang, H.; Zhang, B.; Ji, R.; Gao, B.; Wu, L.; Luo, X.; Xu, G. Characterizing cryptocurrency exchange scams. *Comput. Secur.* **2020**, *98*, 101993. [CrossRef]
37. Badawi, E.; Jourdan, G.V. Cryptocurrencies emerging threats and defensive mechanisms: A systematic literature review. *IEEE Access* **2020**, *8*, 200021–200037. [CrossRef]
38. UmaMaheswaran, S.; Uike, D.; Ramachandran, K.; Tharangini, A.; Suba, T.; Verma, D. The Critical Understanding on the Emerging Threats and Defensive Aspects in Cryptocurrencies using Machine Learning Techniques. In Proceedings of the 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 28–29 April 2022; pp. 1938–1942.
39. Xia, P.; Wang, H.; Luo, X.; Wu, L.; Zhou, Y.; Bai, G.; Xu, G.; Huang, G.; Liu, X. Don't fish in troubled waters! characterizing coronavirus-themed cryptocurrency scams. In Proceedings of the 2020 APWG Symposium on Electronic Crime Research (eCrime), Boston, MA, USA, 16–19 November 2020; pp. 1–14.
40. Bartoletti, M.; Carta, S.; Cimoli, T.; Saia, R. Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact. *Future Gener. Comput. Syst.* **2020**, *102*, 259–277. [CrossRef]
41. Toyoda, K.; Ohtsuki, T.; Mathiopoulos, P.T. Multi-class Bitcoin-enabled service identification based on transaction history summarization. In Proceedings of the 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), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1153–1160.
42. Bartoletti, M.; Pes, B.; Serusi, S. Data mining for detecting Bitcoin ponzi schemes. In Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, Switzerland, 20–22 June 2018; pp. 75–84.
43. Victor, F.; Hagemann, T. Cryptocurrency pump and dump schemes: Quantification and detection. In Proceedings of the 2019 International Conference on Data Mining Workshops (ICDMW), Beijing, China, 8–11 November 2019; pp. 244–251.
44. Vasek, M.; Thornton, M.; Moore, T. Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 3–7 March 2014; pp. 57–71.
45. Baek, U.J.; Ji, S.H.; Park, J.T.; Lee, M.S.; Park, J.S.; Kim, M.S. DDoS attack detection on Bitcoin ecosystem using deep-learning. In Proceedings of the 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), Matsue, Japan, 18–20 September 2019; pp. 1–4.
46. Kharraz, A.; Ma, Z.; Murley, P.; Lever, C.; Mason, J.; Miller, A.; Borisov, N.; Antonakakis, M.; Bailey, M. Outguard: Detecting in-browser covert cryptocurrency mining in the wild. In Proceedings of the World Wide Web Conference, San Francisco, CA, USA, 13–17 May 2019; pp. 840–852.
47. Yin, H.S.; Vatrapu, R. A first estimation of the proportion of cybercriminal entities in the Bitcoin ecosystem using supervised machine learning. In Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 11–14 December 2017; pp. 3690–3699.
48. Chen, W.; Zheng, Z.; Cui, J.; Ngai, E.; Zheng, P.; Zhou, Y. Detecting ponzi schemes on ethereum: Towards healthier blockchain technology. In Proceedings of the 2018 World Wide Web Conference, Lyon, France, 23–27 April 2018; pp. 1409–1418.

49. Jung, E.; Le Tilly, M.; Gehani, A.; Ge, Y. Data mining-based ethereum fraud detection. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 266–273.
50. Chen, W.; Zheng, Z.; Ngai, E.C.H.; Zheng, P.; Zhou, Y. Exploiting blockchain data to detect smart ponzi schemes on ethereum. *IEEE Access* **2019**, *7*, 37575–37586. [CrossRef]
51. Gangwal, A.; Conti, M. Cryptomining cannot change its spots: Detecting covert cryptomining using magnetic side-channel. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 1630–1639. [CrossRef]
52. Ning, R.; Wang, C.; Xin, C.; Li, J.; Zhu, L.; Wu, H. Capjack: Capture in-browser cryptojacking by deep capsule network through behavioral analysis. In Proceedings of the IEEE INFOCOM 2019—IEEE Conference on Computer Communications, Paris, France, 29 April–2 May 2019; pp. 1873–1881.
53. Zimba, A.; Chishimba, M.; Ngongola-Reinke, C.; Mbale, T.F. Demystifying cryptocurrency mining attacks: A semi-supervised learning approach based on digital forensics and dynamic network characteristics. *arXiv* **2021**, arXiv:2102.10634.
54. Alarab, I.; Prakoonwit, S.; Nacer, M.I. Comparative analysis using supervised learning methods for anti-money laundering in Bitcoin. In Proceedings of the 2020 5th International Conference on Machine Learning Technologies, Beijing, China, 19–21 June 2020; pp. 11–17.
55. Farrugia, S.; Ellul, J.; Azzopardi, G. Detection of illicit accounts over the Ethereum blockchain. *Expert Syst. Appl.* **2020**, *150*, 113318. [CrossRef]
56. Goyal, P.S.; Kakkar, A.; Vinod, G.; Joseph, G. Crypto-ransomware detection using behavioural analysis. In *Reliability, Safety and Hazard Assessment for Risk-Based Technologies*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 239–251.
57. Shayegan, M.J.; Sabor, H.R.; Uddin, M.; Chen, C.L. A Collective Anomaly Detection Technique to Detect Crypto Wallet Frauds on Bitcoin Network. *Symmetry* **2022**, *14*, 328. [CrossRef]
58. Hu, H.; Bai, Q.; Xu, Y. Scsguard: Deep scam detection for ethereum smart contracts. In Proceedings of the IEEE INFOCOM 2022—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Virtual, 2–5 May 2022; pp. 1–6.
59. La Morgia, M.; Mei, A.; Sassi, F.; Stefa, J. Pump and dumps in the Bitcoin era: Real time detection of cryptocurrency market manipulations. In Proceedings of the 2020 29th International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, 3–6 August 2020; pp. 1–9.
60. Mirtaheri, M.; Abu-El-Haija, S.; Morstatter, F.; Ver Steeg, G.; Galstyan, A. Identifying and analyzing cryptocurrency manipulations in social media. *IEEE Trans. Comput. Soc. Syst.* **2021**, *8*, 607–617. [CrossRef]
61. Chen, W.; Xu, Y.; Zheng, Z.; Zhou, Y.; Yang, J.E.; Bian, J. Detecting Pump & Dump Schemes on cryptocurrency market using an improved Apriori Algorithm. In Proceedings of the 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE), San Francisco, CA, USA, 4–9 April 2019; pp. 293–2935.
62. Yuan, Q.; Huang, B.; Zhang, J.; Wu, J.; Zhang, H.; Zhang, X. Detecting phishing scams on ethereum based on transaction records. In Proceedings of the 2020 IEEE International Symposium on Circuits and Systems (ISCAS), Sevilla, Spain, 10–21 October 2020; pp. 1–5.
63. Zhang, Y.; Yu, W.; Li, Z.; Raza, S.; Cao, H. Detecting ethereum Ponzi schemes based on improved LightGBM algorithm. *IEEE Trans. Comput. Soc. Syst.* **2021**, *9*, 624–637. [CrossRef]
64. Kumar, N.; Singh, A.; Handa, A.; Shukla, S.K. Detecting malicious accounts on the Ethereum blockchain with supervised learning. In Proceedings of the International Symposium on Cyber Security Cryptography and Machine Learning, Be'er Sheva, Israel, 2–3 July 2020; pp. 94–109.
65. Fan, S.; Fu, S.; Luo, Y.; Xu, H.; Zhang, X.; Xu, M. Smart Contract Scams Detection with Topological Data Analysis on Account Interaction. In Proceedings of the 31st ACM International Conference on Information & Knowledge Management, Atlanta, GA, USA, 17–21 October 2022; pp. 468–477.
66. Nizzoli, L.; Tardelli, S.; Avvenuti, M.; Cresci, S.; Tesconi, M.; Ferrara, E. Charting the landscape of online cryptocurrency manipulation. *IEEE Access* **2020**, *8*, 113230–113245. [CrossRef]
67. Phillips, R.; Wilder, H. Tracing cryptocurrency scams: Clustering replicated advance-fee and phishing websites. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020; pp. 1–8.
68. Wu, J.; Yuan, Q.; Lin, D.; You, W.; Chen, W.; Chen, C.; Zheng, Z. Who are the phishers? phishing scam detection on ethereum via network embedding. *IEEE Trans. Syst. Man Cybern. Syst.* **2020**, *52*, 1156–1166. [CrossRef]
69. Lorenz, J.; Silva, M.I.; Aparício, D.; Ascensão, J.T.; Bizarro, P. 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, New York, NY, USA, 15–16 October 2020; pp. 1–8.
70. Badawi, A.; Al-Haija, Q.A. Detection of money laundering in Bitcoin transactions. In Proceedings of the 4th Smart Cities Symposium (SCS 2021), Online, 21–23 November 2021; pp. 458–464.
71. Baek, H.; Oh, J.; Kim, C.Y.; Lee, K. A model for detecting cryptocurrency transactions with discernible purpose. In Proceedings of the 2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN), Zagreb, Croatia, 2–5 July 2019; pp. 713–717.
72. Wen, H.; Fang, J.; Wu, J.; Zheng, Z. Transaction-based hidden strategies against general phishing detection framework on ethereum. In Proceedings of the 2021 IEEE International Symposium on Circuits and Systems (ISCAS), Daegu, Republic of Korea, 22–28 May 2021; pp. 1–5.

73. Chen, W.; Guo, X.; Chen, Z.; Zheng, Z.; Lu, Y. Phishing Scam Detection on Ethereum: Towards Financial Security for Blockchain Ecosystem. In Proceedings of the IJCAI, Yokohama, Japan, 11–17 July 2020; pp. 4506–4512.
74. Ostapowicz, M.; Żbikowski, K. Detecting fraudulent accounts on blockchain: A supervised approach. In Proceedings of the International Conference on Web Information Systems Engineering, Amsterdam, The Netherlands, 20–24 October 2020; pp. 18–31.
75. Toyoda, K.; Ohtsuki, T.; Mathiopoulos, P.T. Identification of high yielding investment programs in Bitcoin via transactions pattern analysis. In Proceedings of the GLOBECOM 2017—2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–6.
76. CNBC. Crypto Scammers Took a Record $14 Billion in 2021, 6 January 2022. Available online: https://www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2021-chainalysis.html (accessed on 21 December 2022).