Cryptocurrencies as a subject of financial fraud

Małgorzata Kutera[1]

Abstract

PURPOSE: *The main purpose of this paper was to identify the current scope of research on cryptocurrencies as a subject of fraud. Detailed research questions related to the determination of contemporary trends of the conducted research and the definition of potential opportunities for further investigation of this topic. One of the questions also concerned identifying the most common crimes committed using cryptocurrencies.* ***METHODOLOGY:*** *The study is based on a systematic literature review (SLR) of 57 publications available on the Scopus database. A bibliometric and descriptive analysis of selected literature items was carried out. Then, vital thematic clusters were separated, and an in-depth content analysis was performed.* ***FINDINGS:*** *The detailed bibliometric and descriptive analysis showed that cryptocurrencies as a subject of financial fraud are generally a new area of scientific research, although it is developing quite intensively. The relatively small number of publications, compared to other similar areas, also indicates that this topic has not yet been explored widely by scientists, and many different research trends can be created in it. Ultimately, the following key research areas were identified: types of cryptocurrency fraud, crime detection methods, risks related to blockchain technology, money laundering, and legal regulations regarding cryptocurrencies. It was also possible to identify that money laundering is currently the most common fraud. However, it has been pointed out that the second most frequent fraud is financial pyramids based on the Ponzi scheme.* ***IMPLICATIONS:*** *The paper clearly presents the main research trends on using cryptocurrencies in criminal activities. At the same time, it was emphasized that, compared to other research areas, this topic is relatively new. Therefore, there is a wide possibility of exploring not only existing but also undiscovered research trends. In addition, key types of fraud in economic practice have been identified, which is particularly important for financial market participants. It was clearly indicated which transactions bear the highest risk. It is also worth paying attention to the critical timeliness of the topic, as the scale of crimes involving cryptocurrencies has recently*

[1] Małgorzata Kutera, PhD., Assistant Professor at the Jagiellonian University, Institute of Economics, Finance and Management, Prof. S. Łojasiewicza 4, 30-348 Krakow, Poland, e-mail: malgorzata.kutera@uj.edu.pl (ORCID: https://orcid.org/0000-0002-7029-2454).

Received 3 August 2022; Revised 18 September 2022, 9 October 2022; Accepted 20 October 2022.

been growing rapidly. The study confirms the insufficient scope of legal regulations, which are not able to strengthen the security of economic transactions adequately. Therefore, it can be a clear indication for the governments of individual countries or international institutions for further efficient changes to the law. ***ORIGINALITY AND VALUE:*** *The contribution of this study is threefold. It is one of the first research papers showing the results of a systematic literature review (SLR) combined with a bibliographic and in-depth analysis of the content of publications in this field. During the work, the VOSviewer software was also used, which enabled objective identification of the main thematic clusters based on the occurrences and link strength of keywords included in the publications. Secondly, the key types of fraud have been identified that, at the same time, cause the most significant financial loss. This allowed for the establishing of directions for further research, which have profound practical implications for market participants. Some of them relate to the need to develop and implement modern computer applications, allowing for the detection of a wider range of emerging abuses.*

Keywords: *cryptocurrency, bitcoin, blockchain, financial frauds, economic crime, money laundering, Ponzi scheme, financial pyramid, systematic literature review*

INTRODUCTION

Bitcoin was the first cryptocurrency to be created by Satoshi Nakamoto in 2009. Its introduction to the economic market completely revolutionized many existing mechanisms related to the financial market. Some changes related to entire foundations, i.e., defining new economic concepts or changing the current perception of selected macro- and microeconomic processes. The key terms in this context are “cryptocurrency” and “blockchain” related to new technologies. In short, it can be concluded that the first is a generic term for a virtual or digital currency that takes the form of coins or tokens. Cryptocurrencies use blockchain technology (Al-Saqaf & Seidler, 2017). In turn, blockchain is defined as a chained data structure that combines blocks of data and information in chronological order and records the blocks in encrypted form as a distributed ledger that cannot be tampered with or forged. It uses timestamps to identify and record each transaction, so the data are traceable, thereby preventing irreversible modifications to data or information (Lu, 2019). So cryptocurrencies do not require a central authority to validate and settle transactions. Instead, they use only cryptography (and an internal incentive system) to control transactions and manage the supply. Payments are validated by a decentralized network (Gandal, Hamrick, Moore, & Oberman, 2018).

From the very beginning, the essence of blockchain and related cryptocurrencies has been the subject of research by scientists. It is possible to identify many research trends by analyzing the potential application areas of the new technology. Blockchain can be used to decentralize the financial system (Chen & Bellavitis, 2020; Patel, Migliavacca & Oriani, 2022; Sánchez, 2022), to create new forms of nonfungible token (NFT) investments (Regner, Schweizer, & Urbach, 2019), and finally to implement smart contracts (Cong & He, 2019; Hughes, Park, Kietzmann, & Archer-Brown, 2019; Rozario & Vasarhelyi, 2018), which are systems that automatically control digital assets according to arbitrary prespecified rules. There is also an increasing trend of its mass application in accounting and financial reporting of enterprises (Schmitz & Leoni, 2019; Pimentel & Boulianne, 2020; Kokina, Mancha, & Pachamanova, 2017). Therefore, further intensive changes in economic systems caused by this invention should be expected.

Particularly noteworthy is distributed, decentralized, and reliable mechanism of cryptocurrencies, thanks to which they have become a global trading platform (Lin, Wu, Hsu, Tu & Liao, 2019). Unfortunately, these same features have also become attractive to criminals (Fletcher, Larkin & Corbet, 2021). In addition, it is worth mentioning the lack of appropriate legal regulations and related supervisory activities on the part of domestic or international institutions (Irwin & Dawson, 2019; Al-Tawil & Younies, 2020; Lui & Ryder, 2021). All this contributes to the growing use of the cryptocurrency market by criminals financing terrorism, money laundering, and other economic abuses. Cryptocurrencies are under constant threat of attack. Numerous researchers have conducted studies to document and combat crimes, such as:

- Ponzi schemes (Vasek & Moore, 2015; Esoimeme, 2018; Bartoletti, Pes, & Serusi, 2018; Zhang, Kang, Dai, Chen, & Zhu, 2021; Wang, Cheng, Zheng, Yang, & Zhu, 2021);
- money laundering (Levin, O'Brien, & Zuberi, 2015; Rivera, 2019; Hendrickson & Luther, 2022; Bartoletti et al., 2018; Barth, Herath, & Xu, 2020; Broadhead, 2018; van Wegberg, Oerlemans, & van Deventer, 2018; Dupuis & Gleason, 2021; Wronka, 2022);
- mining botnets (Huang et al., 2014; Konoth et al., 2018) and the theft of "brainwallets" (Vasek, Bonneau, Castellucci, Keith, & Moore, 2016).

Thousands of new cryptocurrencies have been introduced in recent years. It is estimated that over 5,100 such assets are currently in operation (Goforth, 2021). The scale and variety of abuses related to it are also growing. The US Federal Trade Commission published a report that presented the latest data on the scale of fraud in the cryptocurrency market (FTC, 2021). It shows that from October 2020 to the end of March 2021, almost 7,000 people fell victim to virtual currency fraud, which resulted in a total loss of more than $ 80 million. For comparison, this sum is nearly 1000% higher than the amount recorded in the corresponding period a year earlier. The report presented by FTC also shows that the median value of the losses suffered was $ 1,900. Global data on the topic can be found in Chainanalysis reports. According to the latest information, the value of frauds and scams in the crypto-assets market in 2021 amounted to $ 14 billion, i.e., almost twice as high ($ 7.8 billion) as the year before (Chainanalysis, 2022). It is also worth paying attention to the scale of money laundering by use of this market. Cybercriminals laundered $ 8.6 billion worth of cryptocurrency in 2021. That represents a 30% increase in money laundering activity over 2020. Cybercriminals have laundered over $ 33 billion worth of cryptocurrency since 2017.

As presented above, the problem is beginning to grow and it significantly affects the security of economic transactions on a global scale. This has been pointed out by both ordinary market participants as well as the governments of individual countries. We are seeing a dynamic increase in global financial flows that are not under any effective control. In connection with the above, it is highly desirable to identify the degree of development and the scope of the current research on the cryptocurrency market in the context of their use for criminal activities. A preliminary analysis of the literature on the subject indicates an existing research gap. There are some studies that present an analysis of the literature on the subject to date (Trozze et al., 2022). The authors have made a scoping review of academic research and grey literature on cryptocurrency fraud. When selecting scientific positions, the Google Scholar search engine was used, and for the remaining publications – the Google search engine. The main purpose of the study was to identify the types of crimes committed with the use of cryptocurrencies. Hence, only those items that contained a description of at least one example of fraud (as of November 2020) were analyzed. As a result of this work, 29 different types of cryptocurrency fraud included in scientific publications and 32 types discussed in the grey literature were distinguished. However, it should be mentioned that only the identification of the types of fraud using cryptocurrencies is insufficient. It is worth making a broader analysis of the literature on the subject in order to define also other areas of research in this field. This article takes that perspective.

The main purpose of the study is, therefore, to identify the current scope of research on cryptocurrencies as a subject of fraud. It will also allow the definition of potential opportunities for further investigation of this topic. To the best of the author's knowledge, it is one of the first studies showing the results of a systematic literature review (SLR) combined with a bibliographic analysis and an in-depth analysis of the content of publications in this field. Detailed research questions are presented later in the study.

This article is structured as follows. The next part deals with the general theoretical background of the subject, with particular emphasis on research conducted in similar areas. Then the research methodology is presented. In this section, research questions are posed. The process of selecting publications for their systematic review is explained in detail, as well as the approach to bibliometric and descriptive analysis. The basic parameters used to distinguish thematic clusters are also presented in this part of the study. The following section shows the results of a systematic review of the literature, including the findings of an in-depth analysis of the content of individual publications. They provide the basis for a discussion on the context of the specific research questions. The last part contains conclusions and presents potential directions for further research in this field.

METHODOLOGY

This study adopted a systematic approach to conducting a literature review to minimize bias and lend scientific value to its results. Systematic literature review (SLR) is a widely recognized scientific method used in social sciences, including management, economics, and finance (Hiebl, 2021; Simsek, Fox, & Heavey, 2021; Sharma & Bansal, 2020). According to the guidelines included in the literature on SLR, the study was divided into the following stages (Jesson, Matheson & Lacey, 2011; Booth, Sutton, & Papaioannou, 2016):

- defining research questions;
- searching for the literature;
- selection of publications using exclusion and inclusion criteria;
- preparation of the final database;
- bibliometric analysis;
- content analysis;
- discussing the results.

At the beginning, three main research questions were defined that set the direction and scope of the systematic literature review, especially in content analysis. The following questions were asked:

RQ1) What are the current state and the primary considerations of research relating to cryptocurrencies as a subject of fraud?
RQ2) What are the most common crimes committed with the use of cryptocurrencies?
RQ3) What could be the future research trends related to cryptocurrencies and financial fraud?

A systematic literature review is crucial in responding to RQ1 and RQ3. In turn, RQ2 is also related to the practical implications of the subject of the study. From the methodological point of view, one of the essential elements of a systematic literature review is an appropriately conducted process of selecting a research sample. The individual steps of eliminating and including in the final set of publications should be based on clear criteria and performed in the correct order. Selected literature items indicate different sampling activities (Sharma & Bansal, 2020; Denyer & Tranfield, 2009; Gaur & Kumar, 2018). However, as a rule, three standard main stages can be distinguished in them:

- identification – it consists in determining a potential group of publications relating to a predefined research problem (Vassar et al., 2017; Booth et al., 2016);
- screening – application of various criteria for inclusion and exclusion of selected items to the final research sample, relating mainly to the substantive content, including also the qualitative assessment of the publication based on content analysis (Booth et al., 2016; Pussegoda et al., 2017; Briner & Denyer, 2012);
- final review sample – determining the definitive set of literature items on the subject being the basis for a detailed analysis from the point of view of the research questions posed. In this respect, there are several guidelines for the minimum dataset size. In the context of the analyzed issue, the minimum sample size should be 50 items (Short, Sharma, Lumpkin & Pearson, 2016; Hiebl, 2021).

A diagram of Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) was used to present the different stages of determining the final set of scientific publications covered by the analysis. This model is one of the most frequently used tools that regulates the sequence of actions performed during the sampling process (Pussegoda et al., 2017; Page et al., 2021; Liberati et al., 2009). Scopus was selected as the key database for the systematic literature review. Before deciding on the choice of the final database, trial tests were also carried out for other databases of scientific publications, especially the Web of Science and ProQuest. However, preliminary results of searching these databases using comparable criteria indicated a smaller number of publications and they included many duplicates. Therefore, it was decided to use Scopus, where the scope of the publication was the largest. The time range of the published scientific items was not limited due to the relatively new subject of scientific research, i.e., cryptocurrencies. An interesting aspect was also the identification of the oldest publications in this field.

The first stage of searching the database and selecting items was determining the keywords appropriate for the research subject. This collection includes cryptocurrencies and crypto assets (crypto *), bitcoin, Ethereum, fraud, crime, scam, and abuse. The first four keywords generally refer to cryptocurrencies and their two most popular and longest-functioning types in the market. The following four keywords are a combination of the most common terms related to financial fraud in the literature. The "Article title, abstract, keywords" area was selected as the reference database for the search. As a result of the database search, 841 publications meeting these criteria were identified.

Then, the subject area had to be narrowed down due to its substantive nature. In this regard, two sites were selected: "business, management, and accounting" and "economics, econometrics, and finance." The scope of the publication was 106 items. Another criterion was to narrow the area of analysis to four types of documents: "article," "conference paper," "book chapter," and "book." The database identified 102 publications. Of these, all articles still in print were discarded, and the focus was solely on the completed items. As a result of the database search, 95 scientific publications were finally included in the collection, and the full search criteria were as follows:

(TITLE-ABS-KEY (crypto*) OR TITLE-ABS-KEY (bitcoin) OR TITLE-ABS-KEY (ethereum) AND TITLE-ABS-KEY (fraud) OR TITLE-ABS-KEY (crime) OR TITLE-ABS-KEY (scam) OR TITLE-ABS-KEY (abuse)) AND (LIMIT-TO (SUBJAREA , "BUSI") OR LIMIT-TO (SUBJAREA , "ECON")) AND (LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "ch") OR LIMIT-TO (DOCTYPE , "bk")) AND (LIMIT-TO (PUBSTAGE , "final")).

The next stage was verifying the titles and abstracts of all 95 bibliographic items to determine which of them relate to the research questions posed. The mainstream research was supposed to concern cryptocurrencies in the context of fraud committed. At this stage, a complete double analysis of titles and abstracts was performed to eliminate the risk of confusion. Thirty-eight publications were rejected. For research purposes, the final collection was 57 literature items. The eliminated publications mainly concerned the possible innovative applications of blockchain technology related to the cryptocurrency market in other areas of life (medicine, education).

The summary of the entire process of selecting the research sample is the following PRISMA diagram presenting the various stages of the elimination of bibliographic items (Figure 1).

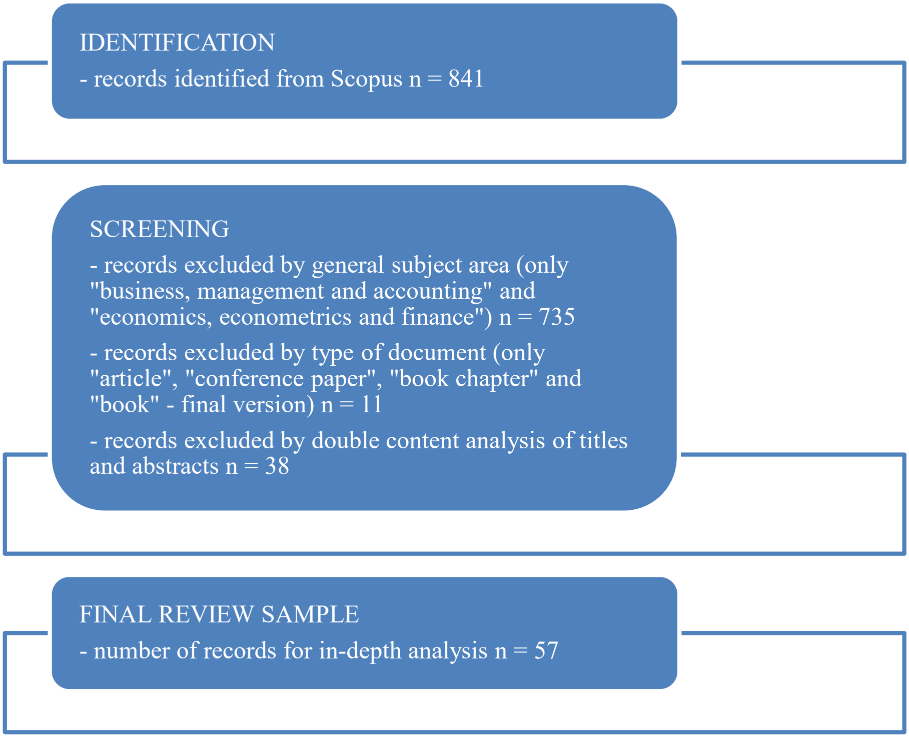
IDENTIFICATION
- records identified from Scopus n = 841
SCREENING
- records excluded by general subject area (only "business, management and accounting" and "economics, econometrics and finance") n = 735
- records excluded by type of document (only "article", "conference paper", "book chapter" and "book" - final version) n = 11
- records excluded by double content analysis of titles and abstracts n = 38
FINAL REVIEW SAMPLE
- number of records for in-depth analysis n = 57

Figure 1. PRISMA diagram – selection of the research sample

In the next stage, bibliometric and descriptive analyses were made to present the primary data on the literature on this subject. The key verification criteria concerned publication trends in particular years, types of these publications, the most popular journals, authors, their affiliation, and countries of origin. The publications were also analyzed in terms of their levels of citation. Using the tools built into the Scopus database, a ranking of the most frequently cited literature items from the collection included in the final analysis was prepared. In this way, it was possible to identify critical publications that were most often included by other authors dealing with similar issues.

The last element was the in-depth content analysis. The starting point for organizing the substantive criteria of this analysis was the verification of potential clusters. Therefore, a network analysis was performed using the VOSviewer 1.6.18 Software. The data was extracted directly from Scopus, including all necessary information (author, title, abstract, keywords, publication year, affiliation, etc.), and then imported to VOSviewer to create the co-occurrence network to identify the main aspects of the discussion. The most crucial element in this respect was the analysis of the co-occurrence network of keywords to distinguish clusters. The key parameters used to define the network of connections are presented in Table 1.

Table 1. Essential parameters for identifying the co-occurrence network of keywords

Parameter	Settings
Type of analysis	Co-occurrence
Unit of analysis	All keywords
Counting method	Full counting
Minimum number of occurrences of a keyword	5
Number of keywords to be selected	10

Subsequently, each literature item within the individual clusters was read, and an in-depth content analysis was performed. A narrative approach was used during this verification, and significant substantive findings relating to the research questions were presented.

RESULTS

The first element is a detailed bibliometric and descriptive analysis. The subject of cryptocurrencies in the context of crime is relatively new compared to other research areas related to management, economics, and finance. Figure 2 presents the evolution of the number of publications in this field. As mentioned above, no filters related to time constraints were assumed when searching the Scopus database. The results, therefore, present the full range of literature on the subject.

One of the analysis's most interesting elements was identifying the oldest publications on cryptocurrencies used as a potential fraud tool. The above chart shows that in 2014 one such item was published. After that, only individual publications were identified over the next several years. It was only in 2018 that higher growth dynamics can be observed – eleven such items were published then. A similar trend continued in the following years (12, 15, and 12 publications in 2021). The chart does not present data from 2022, as the information does not include the whole year and it would distort the conclusions from the comparative analysis. This implies that after the first cryptocurrency was introduced to the market, at least a few years had to pass before it became the object of interest to scientists. It is also clear that in the early years, cryptocurrencies were not identified as potential financial crime tools.

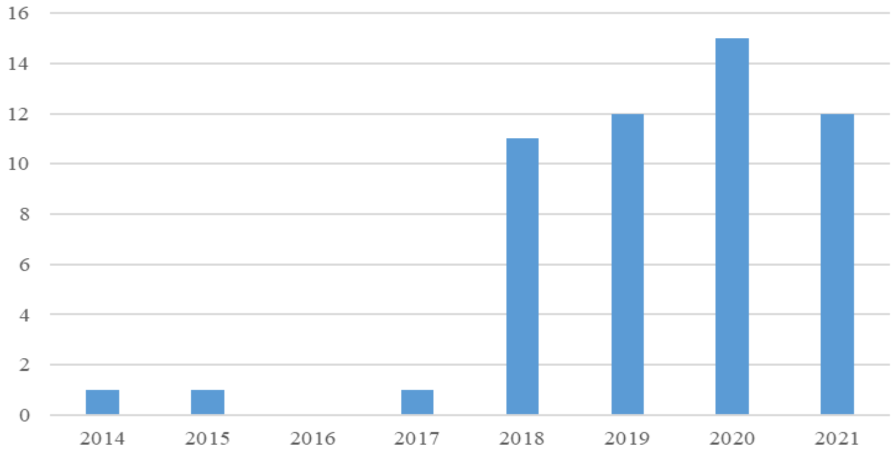

Figure 2. Number of publications in respective years

Another aspect of bibliometric verification is the publication type and the most famous journals. The data show that among the entire group of 57 literature items, the most significant number is of scientific articles (36) and publications in conference materials (14). Trace amounts refer to chapters in books or complete monographs. A summary of these data is presented in Figure 3.

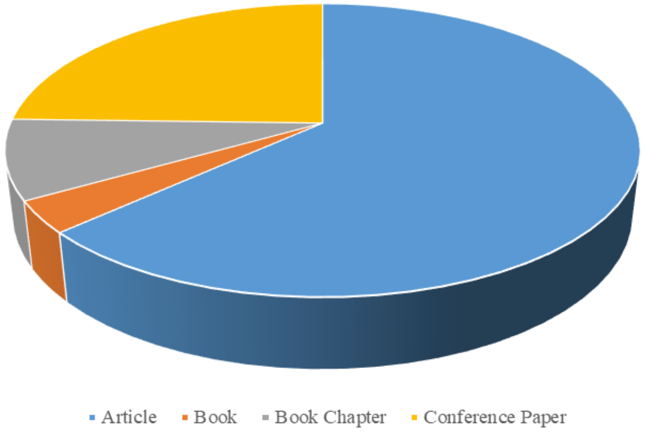

Figure 3. Types of publications

The publications appeared in a total of 42 different journals and conference materials. The analysis showed that articles in this field are most often published in the Journal of Money Laundering Control, which immediately suggests the essence of the research issue and the most common type of fraud in the context of cryptocurrency trading. A total of 10 publications were identified in this journal. The following items are publications in conference materials relating to the IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2020, and four more journals. Two elements of the literature on the subject were identified. The rest are single publications in 36 different journals. It is immediately noticeable that there is one top place dealing with the issue of cryptocurrencies in the context of economic fraud. Table 2 presents the primary sources of publications in this field.

Table 2. Most common journals

Title	Number of articles
Journal of Money Laundering Control	10
IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2020	3
Research in International Business and Finance	2
Journal of Financial Crime	2
Journal of Advanced Research in Law and Economics	2
International Journal of Recent Technology and Engineering	2

Considering the number of publications issued by individual authors, it is difficult to identify a leading scientist specializing in this subject. Only five people with two publications on using cryptocurrencies in financial frauds can be distinguished – Esoimeme, Falker, Moore, Teichmann, and Wronka. It is worth pointing out that all of their scientific articles are about money laundering with crypto-assets and have been published in the Journal of Money Laundering Control. Most researchers dealing with this subject come from the United States, Great Britain, and China. Due to the large dispersion of publications issued by individual authors, it is also impossible to indicate specific research centers related to the affiliation that would play a leading role in scientific research on this subject.

Table 3 presents the ranking of publications from their citation point of view. It includes all items for which more than 10 citations were identified. In total, for the entire set of 57 items, 921 citations were established in other scientific publications, of which 11 articles did not receive any citations in the analyzed period of 2018-2022.

Table 3. Most cited publications

Title	Authors	Number of citations
Price manipulation in the Bitcoin ecosystem	Gandal N., Hamrick J.T., Moore T., Oberman T.	259
Blockchain technology innovations	Ahram T., Sargolzaei A., Sargolzaei S., Daniels J., Amaba B.	227
Data mining for detecting bitcoin Ponzi schemes	Bartoletti M., Pes B., Serusi S.	109
Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin	van Wegberg R., Oerlemans J.J., van Deventer O.	32
News sentiment in the cryptocurrency market: An empirical comparison with Forex	Rognone L., Hyde S., Zhang S.S.	28
An Evaluation of Bitcoin Address Classification based on Transaction History Summarization	Lin Y.J., Wu P.W., Hsu C.H., Tu I.P., Liao S.W.	25
Multi-Class Bitcoin-Enabled Service Identification Based on Transaction History Summarization	Toyoda K., Ohtsuki T., Mathiopoulos P.T.	24
Bitcoin, life coin, name coin: The legal nature of virtual currency	Kirillova E.A., Pavlyuk A.V., Mikhaylova I.A., Zulfugarzade T.E., Zenin S.S.	24
Underpricing in the cryptocurrency world: evidence from initial coin offerings	Felix T.H., von Eije H.	22
The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments	Broadhead S.	13
Is bitcoin a waste of resources?	Williamson S.	12
Tracing Cryptocurrency Scams: Clustering Replicated Advance-Fee and Phishing Websites	Phillips R., Wilder H.	12
Pricing Efficiency and Arbitrage in the Bitcoin Spot and Futures Markets	Lee S., Meslmani N.E., Switzer L.N.	11
Countering money laundering and terrorist financing: A case for bitcoin regulation	Fletcher E., Larkin C., Corbet S.	10

When analyzing the above results, three leading items of the most significant substantive importance with more than 100 citations should be identified. They mainly relate to manipulating the bitcoin exchange rate or its use to build a financial pyramid (Ponzi scheme).

The next stage of the systematic literature review is the in-depth content analysis of the collection of publications from the point of view of achieving the main goal and the research questions posed. The starting point for this analysis was the identification of potential substantive clusters. As mentioned earlier, VOSviewer Software was used to create the co-occurrence network using all keywords to identify the main aspects of the publications.

As part of the selection process presented in the methodology section, a total of 322 keywords were identified, of which only 10 met the assumed criteria. The number of occurrences and total link strength for the most important keywords are presented in Table 4.

Table 4. Occurrences and link strength of keywords

Keyword	Occurrences	Total link strength
bitcoin	30	53
blockchain	19	52
cryptocurrency	21	44
crime	11	30
chromium compounds	5	18
Ethereum	6	18
money laundering	10	16
block - chain	5	15
electronic money	5	13
cryptocurrencies	6	7

Generally, three clusters focused on the following keywords were identified:

- bitcoin – electronic money, cryptocurrencies;
- blockchain – crime, chromium compounds, Ethereum, block – chain;
- cryptocurrency – money laundering.

The results are presented in Figure 4, which shows network visualization. In addition, the density visualization in Figure 5 was also included to provide a complete presentation of the selected clusters.

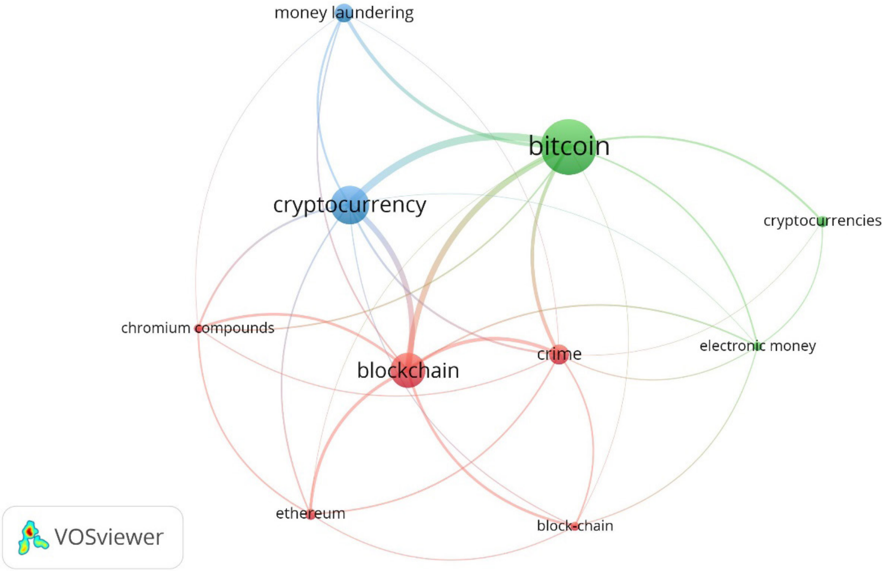

Figure 4. Co-occurrence analysis of the authors' keywords

Source: own study using VOSviewer 1.6.18.

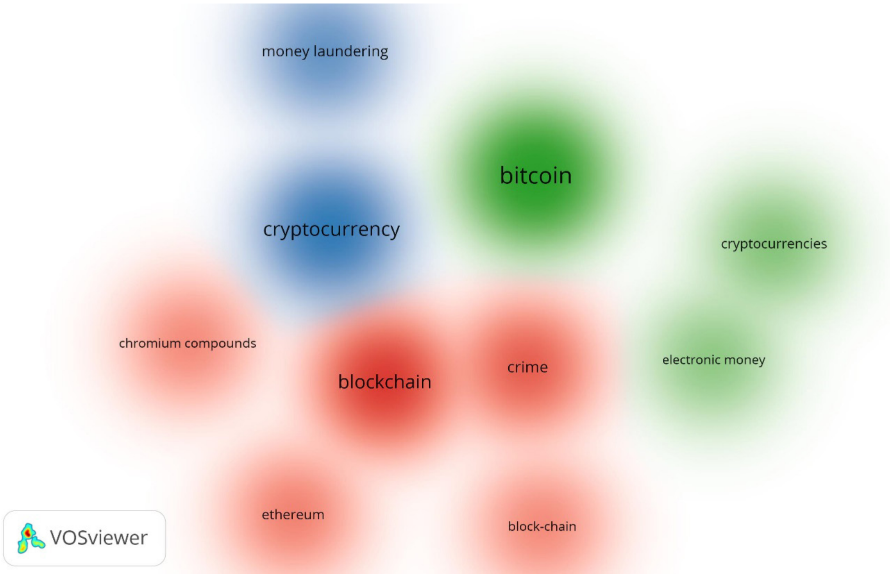

Figure 5. Clusters of the authors' keywords

Source: own study using VOSviewer 1.6.18.

Cluster "Bitcoin"

Bitcoin as the oldest cryptocurrency and various aspects related to its functioning, is by far the most frequently discussed topic in the literature on the subject. Many authors emphasize that the perception of bitcoin has significantly evolved and is now a normally functioning asset in financial markets. Therefore, Teo and Low (2018) pointed out that it is necessary to redefine the concept of "money" as an asset and define its protection principles. They showed various legal aspects related to defining this concept and the resulting risks in investment practice. It was especially emphasized that the main threat in this regard is hacking.

A large part of the publication shows examples of possible illegal use of bitcoin for various crimes, including money laundering (Esoimeme, 2018; Bartoletti et al., 2018; Barth et al., 2020; Broadhead, 2018, van Wegberg et al., 2018). Esoimeme (2018) indicates that bitcoin creates hitherto unknown opportunities for marketing funds from illegal sources, much more significant than traditional money transfers. For example, the Mavrodi Mondial Movement (MMM) pyramid scheme operating in recent years in Nigeria and the risks associated with new payment methods are given.

Ponzi scheme-based financial pyramids are one of the most commonly used frauds in the context of bitcoin, with the longest tradition in the market. It is noted by Bartoletti, Pes, and Serusi (2018), Zhang, Kang, Dai, Chen, and Zhu (2021), Wang, Cheng, Zheng, Yang, and Zhu (2021). They build a network of investors, where the profits paid to the first participants of the system come from payments made by subsequent investors and not from the funds generated by the system. The authors emphasize that immediately after the introduction of bitcoin in 2009, there were signs of building financial pyramids with its use. At the same time, they proposed various techniques for detecting bitcoin addresses directly related to Ponzi schemes, allowing early identification of this type of fraud. The method involves experimenting with different machine learning algorithms and evaluating their effectiveness using standard validation protocols and performance metrics. In turn, Wang, Cheng, Zheng, Yang, and Zhu (2021) proposed a method for detecting pyramid schemes based on oversampling Long Short-Term Memory. Account features and code features are extracted from contract call information and contract codes, and the two components are combined to detect Ponzi scheme smart contracts.

Analyzing bitcoin addresses and their associated transaction types is also of interest to Lin, Wu, Hsu, Tu, and Liao (2019). They point out that the ability to identify addresses associated with criminal activities is becoming the most critical issue in the cryptocurrency network. They experimented with building a classification model for detecting abnormality of bitcoin network addresses. These features include various high orders of moments of transaction time, which summarizes the transaction history in an efficient way. This allows the addresses associated with the scams to be identified. A modern tool for detecting suspicious bitcoin accounts was also proposed by Sun, Xiong, Yiu, and Lam (2019), who developed the BitVis system. With it, cryptocurrency investors can easily filter transactions on demand, interact with trading networks to find helpful information, and analyze the behavior of bitcoin accounts. The mechanism may also be successfully used by authorities regulating financial markets.

A tool popularly known as honeypot (Torres, Baden & State, 2020) can also play a similar role. This particular trap is aimed at detecting attempts at the unauthorized use of the system or obtaining data. Most often, it consists of a computer, data, and a separate area of the local network, which pretends to be a real network but are isolated from it and adequately secured. From the outside, this construction looks like it contains information or a resource that could be a potential target of a cybercriminal. Another publication that presents the potential possibilities of preventing fraud with bitcoin is the study on the innovative solution proposed by Toyoda, Ohtsuki, and Mathiopoulos (2018). Scientists implemented a multi-faceted scheme for identifying services based on bitcoin addresses by analyzing the history of transactions. It allows distinguishing seven significant services: regular exchange, faucet, gambling, investment scam, marketplace, mining pool, and mixer. The model provides 72% accuracy and it has been tested on over 26,000 bitcoin addresses. In turn, Lorenz, Silva, Aparício, Ascensão, and Bizarro (2020) conducted experiments to detect illegal activity in a set of bitcoin transactions. They studied the detection ability of the machine learning model and proved that unsupervised anomaly detection methods have poor results.

Interesting research in the context of bitcoin has also been presented by Barth, Herath, and Xu (2020). These scientists were looking for answers as to whether, and to what extent, ethical aspects affect the valuation of cryptocurrencies. To this end, they measured the intensity of the use of ethical and unethical words in the discussion of bitcoin on Twitter and its valuation. They discovered that the frequency of an unethical discussion about bitcoin is negatively associated with its price. In contrast, the frequency of an ethical debate is positively associated with its price.

Cluster "Blockchain"

The publications belonging to this cluster mainly concern blockchain as a new technology covering, among other things, the cryptocurrency market and they draw attention to various associated risks. It is assumed that this solution completely revolutionized the existing digital world and brought an entirely new perspective on its security, flexibility, and efficiency (Srivasthav, Maddali, & Vigneswaran, 2021). On the one hand, it is emphasized that blockchain allows for a completely different dimension of transactions or exchange of goods and services. However, its further development depends to a large extent on regulatory changes protecting against cybercrimes and financial frauds (Ahram, Sargolzaei, Daniels & Amaba, 2017).

The WannaCry ransomware attack that took place in May 2017 was given as an example of a new type of crime involving blockchain-based cryptocurrency payment transactions (Turner, McCombie, & Uhlmann, 2019). It was a global hacking attack that involved computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the bitcoin cryptocurrency. At the same time, the authors developed a model for collecting and analyzing data related to inflows and outflows of bitcoin-related ransomware transactions. Bitcoin transactions form graph networks and enable the construction of a target network model for collecting, analyzing, and sharing intelligence with multiple stakeholders. It would therefore be possible to counter such attacks more quickly and effectively in the future.

Karapapas, Pittaras, Fotiou, and Polyzos (2020) draw attention to the increased risk of hacker attacks using blockchain technology. The authors clearly showed how technology could be used to launch ransomware campaigns as a service. They proved that criminals could transact with related parties and victims without revealing their identity and with multiple privacy guarantees. The scale of cyber-attacks in cryptocurrency trading and the use of technology was also the subject of research by Caporale, Kang, and Spagnolo (2020). They thoroughly analyzed hacking attacks on the four most popular cryptocurrencies. They confirmed their significant negative financial consequences and, at the same time, pointed to the need to increase research in this field. They considered the precise understanding of the mechanisms of cyber-attacks to be crucial in the fight against this phenomenon.

With the development of blockchain and the cryptocurrency market, the scale of abuse related to the simple theft of these assets has also increased. Only the tools used by criminals have changed. These scams operate on visually similar but seemingly unrelated websites advertised by malicious social media accounts. With the help of such websites and social media accounts, they often perpetrate fraud or act as phishing sites. For example, Phillips and Wilder (2020) analyzed selected data online and based on blockchain technology. Using the clustering technique, they developed a typology of prepayment and phishing scams. It turned out that the same entities carried out very similar scams in their online activities and using blockchain.

Cluster "Cryptocurrency"

The vast majority of publications in this field see the problem of using cryptocurrencies for various crimes, including primarily money laundering. Levin, O'Brien, and Zuberi (2015) explicitly point out that until recently, the bitcoin market was considered a "virtual Wild West for drug dealers and other criminals." At the same time, they pointed out that the support for this currency is constantly growing, and it has become a global virtual asset. The regulations governing this market do not keep up with the practice and seem unclear. The authors cite examples of American administrative proceedings against operators of platforms on which cryptocurrency trading is carried out and analyze the current state of legal regulations in this field in the USA.

The issue of appropriate regulation was also raised by Irwin and Dawson (2019), who specifically dealt with the law of payment methods. The authors identified the current legal status in Australia, Europe, and America and, at the same time, indicated potential limitations in their application on a global scale. In addition, they highlighted the ineffectiveness of the implemented solutions, which also have a negative impact on the possibility of prosecuting criminals. One of the reasons they mentioned is the lack of a legal, universally binding definition of bitcoin.

It is also emphasized that countries that give up cash transactions entirely are not much less vulnerable to money laundering crimes (Rivera, 2019; Hendrickson & Luther, 2022). In this case, virtual transactions, including those related to cryptocurrencies, are used on a larger scale. After all, popular cryptocurrencies like bitcoin are close substitutes for cash. In addition, they offer a higher level of financial anonymity and thus allow transactions with a lower risk of detection than traditional digital payments. Consequently, all efforts to eliminate cash from circulation strongly drive criminals towards cryptocurrencies.

Experts indicate that a substantial restriction of trading in cryptocurrencies is not the solution for the future either, because they appeared as a natural consequence of the intensive development of technology. However, it is essential to introduce global legal regulations limiting their criminal use (Al-Tawil & Younies, 2020). Liechtenstein is quite an active country in this context (Teichmann & Falker, 2020; 2021). Particular guidelines have recently been introduced regulating this market ("The Liechtenstein Blockchain Act"), preventing money laundering above all. New regulations were also introduced relatively quickly in Malta (Buttigieg & Sapiano, 2020). Teichmann and Falker (2020) also presented specific methods used by people involved in money laundering using crypto assets. The qualitative research included 10 presumed money-laundering people and 18 anti-money-laundering experts.

Quite an exciting publication was prepared by Dupuis and Gleason (2021). The authors presented the possibilities and limitations of the cryptocurrency market as a place for money laundering. They performed an in-depth analysis of the currently available exchange mechanisms of these assets in light of the existing legal regulations. The illegal use of cryptocurrencies was investigated through Kane's regulatory dialectical paradigm and it eventually identified six potential tools used by criminals.

A similar topic was taken up by Lui and Ryder (2021). They classified the mechanisms of using cryptocurrencies in financial crimes and analyzed the relevant legal provisions in Great Britain. There has also been an attempt to identify the current loopholes in the regulatory systems that are most often exploited by fraudsters. The authors emphasized that, despite the efforts of the Financial Action Taskforce, the legal system does not keep up with the development of technology, and harmonized global actions are needed in this regard.

Potential money laundering techniques using cryptocurrencies were also presented by Wronka (2022). He classified the most common fraud mechanisms and patterns and highlighted the changing cryptocurrency market that brings new opportunities for fraud. The author also analyzed the extent to which EU and national regulations can counteract this phenomenon, bearing in mind the security of the financial market. In verifying domestic law, he dealt mainly with the legal provisions in force in Germany, Great Britain, and Switzerland. Findings suggested that relatively lenient laws exist in Switzerland and Germany, while Great Britain has the most stringent regulations.

The directions of changes in the law in the context of the security of cryptocurrency trading were also presented by Fletcher, Larkin, and Corbet (2021). They performed an in-depth analysis of the regulations in the American market. The authors distinctly indicated that bitcoin and other crypto-assets should be classified as a technology with financial components and regulated as a part of the growing FinTech industry. In turn, Riley (2021) reviewed current Chinese law, with particular emphasis on the new Chinese Cryptography Law.

DISCUSSION

The bibliometric and descriptive analysis summary presented above made it possible to partially answer the first research question regarding the state of scientific publications on cryptocurrencies as a subject of fraud. There has been an increased interest in this topic for several years.

The detailed content analysis of the literature items made it possible to indicate the main research trends, identify the most frequently committed frauds with the use of cryptocurrencies and define future research directions, which are closely related to the research questions posed. The starting point was the identification of three keyword-based clusters. The verification of the publications included in individual groups indicated some thematic specialization.

Within the bitcoin cluster, the most significant number of studies presenting various types of crimes committed with its use and possible techniques for detecting these abuses were identified. Some publications also referred to the need to redefine critical concepts related to cash turnover or ethics. Cluster "blockchain" clearly focuses on new technology and the resulting risks. On the other hand, the group of studies in the field of cryptocurrencies mainly refers to issues related to money laundering and changes in international and national legal regulations regarding cryptocurrency trading. Figure 6 summarizes the identified vital research trends.

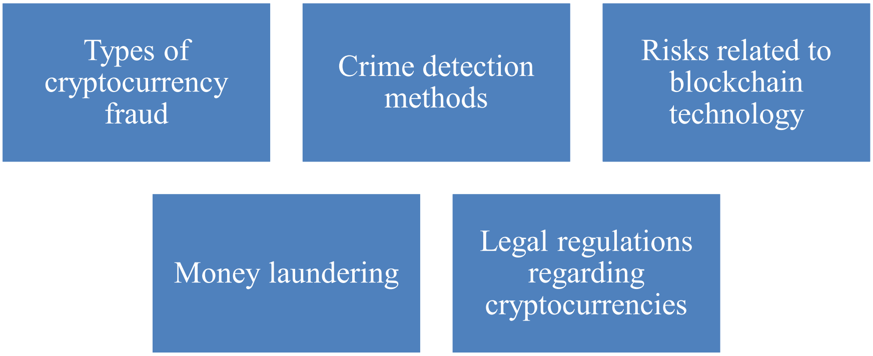
Types of cryptocurrency fraud
Crime detection methods
Risks related to blockchain technology
Money laundering
Legal regulations regarding cryptocurrencies

Figure 6. Main research areas in scientific publications

The two main types of economic crime related to the cryptocurrency market are money laundering and financial pyramids based on the Ponzi scheme. All authors point out that this market offers new and unprecedented possibilities for transferring funds from illegal sources. This is facilitated by certain anonymization of transactions and the lack of clear legal regulations. As soon as the formalized framework for the organized cryptocurrency trading market, including mainly bitcoin at first, emerged, criminals found new opportunities for money laundering. This type of abuse is by far the most common in the cryptocurrency context (Esoimeme, 2018; Levin et al., 2015; Rivera, 2019; Hendrickson & Luther, 2022; Bartoletti et al., 2018; Barth et al., 2020; Broadhead, 2018; van Wegberg et al., 2018; Dupuis & Gleason, 2021; Wronka 2022).

However, attention should be paid to the second, quite a strong trend of publications on the use of the cryptocurrency market to build Ponzi schemes (Esoimeme, 2018; Bartoletti et al., 2018; Zhang et al., 2021; Wang et al., 2021). The crimes of the financial pyramid have been known in the market for many years and they have always aroused a lot of emotions, mainly due to the scale of actions of selected fraudsters and the wide range of victims. The very name of the type of fraud comes from Charles Ponzi, an Italian immigrant living in the United States. In 1920, he built the first financial pyramid (based on the international reply coupons IRC). Since then, this type of fraud has systematically appeared in the market. One of the largest frauds of this type in the economic history of the world is the financial pyramid of Bernard L. Madoff, a well-known American stock exchange player. The number of victims exceeded fourteen thousand people and the losses were estimated at tens of billions of dollars (Kutera, 2016). The cryptocurrency market offers new opportunities in this regard, although the essence of the crime has remained unchanged. It was presented in detail by Wang, Cheng, Zheng, Yang, and Zhu (2021), who described the fraud mechanism using the example of PlusToken. However, there are more examples: the OneCoin-based pyramid operating in 2014-2017 or BitConnect (2016-2018).

Another area of research is the methods of detecting cryptocurrency scams. Most researchers here focus on various ways of verifying bitcoin addresses and identifying those that bear the hallmarks of criminal activity (Bartoletti et al., 2018; Lin et al., 2019; Toyoda et al., 2018). Other proposals relate to machine learning models (Wang et al., 2021; Lorenz et al., 2020) or completely original solutions (Sun et al., 2019; Torres et al., 2020). In this context, everyone emphasizes that the capabilities of blockchain technology can also contribute to a more effective fight against economic crime related to cryptocurrencies. This trend of research also applies to the IT sector, where you can see a growing number of publications describing the use of so-called smart contracts. Therefore, it seems that the subject of creating various application tools supporting fraud detection in the blockchain environment will be a separate and stringent research stream.

The analysis of the content of publications regarding various risks arising from the use of blockchain technology and their potential impact on the cryptocurrency market showed that the main problem is hacker attacks. Selected studies presented examples of such situations and identified the scale of financial losses (Turner et al., 2019; Broadhead, 2018). The most significant illegal acquisitions of cryptocurrencies as a result of imperfect information systems took place, for example, on Mt. Gox, where the size of the financial damage was estimated at $ 473 million. Other examples include the hacking attacks on the Bitfinex exchange in August 2016 (total losses amounted to $ 72 million), PolyNetwork in August 2021 ($ 600 million), and Zaif in September 2018 ($ 62 million). Some publications in this area also presented more technical aspects related to the actual carrying out of attacks and analyzed the main IT tools used in the crime (Karapapas et al., 2020; Caporale et al., 2020; Phillips & Wilder, 2020).

The last highlighted research area is that of legal regulations regarding cryptocurrencies and their impact on the security level of this market. The analysis covers both global and national levels. The authors identified the current state of the law and the desired directions of its changes. The regulations applied in the United States (Levin et al., 2015; Fletcher et al., 2021), Great Britain (Lui & Ryder, 2021; Wronka, 2022), China (Riley, 2021), Australia (Irwin & Dawson, 2019), Germany and Switzerland (Wronka, 2022) and in smaller countries such as Liechtenstein (Teichmann & Falker, 2020; 2021) and Malta (Buttigieg & Sapiano, 2020). In some cases, broader international comparative analyzes were carried out, which allowed for more profound conclusions. In general, attention was drawn to the urgent need to develop and implement some global standards regulating the cryptocurrency market. The rules applied at the national level are insufficient to protect investors fully. Crypto-asset transactions, by their nature, involve transnational cash flows.

CONCLUSION

The main purpose of this paper was to identify the current scope of research on cryptocurrencies as a subject of fraud. Ultimately, 57 publications were selected for the systematic review of the literature. The detailed bibliometric and descriptive analysis showed that it is generally a new area of scientific research, although it is developing quite intensely. The relatively small number of publications compared to other similar areas also indicates that this topic is not yet explored widely by scientists, and many different research trends can be created within it.

In turn, an in-depth analysis of the content made it possible to find answers to the specific research questions. They mainly referred to identifying the most critical trends in the current research on cryptocurrencies in the context of financial fraud and the definition of potential opportunities for further investigation of this topic. The starting point in this part of the study was the identification of three thematic clusters and more detailed areas of analysis within them. Ultimately, the following key research trends were identified: types of cryptocurrency fraud, crime detection methods, risks related to blockchain technology, money laundering, and legal regulations related to cryptocurrencies. One of the questions also concerned the practical implications of the research area, namely identifying the most common crimes committed with the use of cryptocurrencies. These include money laundering and financial pyramids based on the Ponzi scheme.

The contribution of this study is threefold. It is one of the first research papers showing the results of a systematic literature review (SLR) combined with a bibliographic and in-depth analysis of the content of publications in this field. This is all the more important as the scale of crimes involving cryptocurrencies is growing yearly, which is also mentioned in this study. Secondly, the key types of fraud have been identified that, at the same time, cause the most significant financial loss. This allowed for the establishing of directions for further research, which have profound practical implications for market participants. The most important issues that should be included are:

- desired changes in the field of international and national legal regulations regarding cryptocurrency trading, which on the one hand, would increase the security of investors, but at the same time, would not inhibit the natural development of new solutions emerging along with the dynamic technological development;
- in-depth research on identifying possible types of fraud committed using cryptocurrencies, mainly to build effective mechanisms to combat these phenomena. In this respect, cooperation of specialists in various fields, for example, financiers and IT specialists, would be desirable;
- creating and analyzing various application tools supporting fraud detection in the blockchain environment.

However, there are also limitations to this study. Regarding the research methodology, the Scopus database does not allow the analysis of all available publications related to the topic (including studies only in paper form). Moreover, only items published in English were taken into account during the selection of articles. Various reports prepared by organizations dealing with the analysis of the cryptocurrency market or institutions responsible for shaping legal regulations in this field were also not taken into account. The main goal of the article was closely related only to scientific publications. It is also worth mentioning the time limit. The selection of the items in the literature on the subject was made as of July 2022. Therefore, the analysis did not cover the latest publications, which may be important in the context of the dynamic development and changes that have taken place on the cryptocurrency market in the recent period of time. Despite this, the author believes the study will be a helpful resource for current and future scholars interested in addressing the most critical connections between cryptocurrencies and financial crimes.

References

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). *Blockchain technology innovations*. Paper presented at the 2017 IEEE Technology and Engineering Management Society Conference, TEMSCON 2017, 137-141. https://doi.org/10.1109/TEMSCON.2017.7998367

Al-Saqaf, W., & Seidler, N. (2017). Blockchain technology for social impact: Opportunities and challenges ahead. *Journal of Cyber Policy*, *2*(3), 338–354. https://doi.org/10.1080/23738871.2017.1400084

Al-Tawil, T.N., & Younies, H. (2020). The implications of the Brexit from the EU and bitcoin. *Journal of Money Laundering Control*, *24*(1), 137-149. https://doi.org/10.1108/JMLC-05-2020-0050

Anagnostiy, E., So, E., Vallabhaneni, P., Abedine, A., & Hayes, C.B. (2020). CFTS jurisdiction over cryptocurrency: Implications for industry participants. *Banking Law Journal*, *137*(2), 63-69. Retrieved from https://www.hklaw.com

Barth, J.R., Herath, H.S.B., Herath, T.C., & Xu, P. (2020). Cryptocurrency valuation and ethics: A text analytic approach. *Journal of Management Analytics*, 367-388. https://doi.org/10.1080/23270012.2020.1790046

Bartoletti, M., Pes, B., & Serusi, S. (2018). *Data mining for detecting bitcoin Ponzi schemes*. Paper presented at the Crypto Valley Conference on Blockchain Technology, CVCBT 2018, 75-84. https://doi.org/10.1109/CVCBT.2018.00014

Booth, A., Sutton, A., & Papaioannou, D. (2016). *Systematic Approaches to a Successful Literature Review* (2nd ed.). London: SAGE.

Briner, R.B., & Denyer, D. (2012). A systematic review and evidence synthesis as a practice and scholarship tool. In D.M. Rousseau (Ed.), *The Oxford Handbook of Evidence-Based Management* (pp. 112-129). Oxford: Oxford University Press.

Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. *Computer Law and Security Review*, *34*(6), 1180-1196. https://doi.org/10.1016/j.clsr.2018.08.005

Buttigieg, C.P., & Sapiano, G. (2020). A critical examination of the VFA framework: The VFA agent and beyond. *Law and Financial Markets Review*, *14*(1), 48-58. https://doi.org/10.1080/17521440.2019.1640421

Caporale, G.M., Kang, W., Spagnolo, F., & Spagnolo, N. (2020). Non-linearities, cyber-attacks, and cryptocurrencies. *Finance Research Letters*, *32*. https://doi.org/10.1016/j.frl.2019.09.012

Chainanalysis. (2022). *The 2022 Crypto Crime Report: Original data and research into cryptocurrency-based crime*, February 2022. Retrieved from https://go.chainalysis.com

Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights*, *13*. https://doi.org/10.1016/j.jbvi.2019.e00151

Cong, L.W., & He, Z. (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies*, *32*(5), 1754-1797. https://doi.org/10.3386/w24399

Denyer, D., & Tranfield, D. (2009). Producing a systematic review. In D.A. Buchanan & A. Bryman (Eds.), *The SAGE Handbook of Organizational Research Methods* (pp. 671-689). London: SAGE.

Dupuis, D., & Gleason, K. (2021). Money laundering with cryptocurrency: Open doors and the regulatory debate. *Journal of Financial Crime*, *28*(1), 60-74. https://doi.org/10.1108/JFC-06-2020-0113

Elwell, C.K., Maureen Murphy, M., & Seitzinger, M.V. (2014). Bitcoin: Questions, answers, and analysis of legal issues. In *Money, Economics, and Finance: Developments, Analyses and Research* (pp. 1-24). Retrieved from https://digital.library.unt.edu

Esoimeme, E.E. (2020). Identifying and reducing the money laundering risks posed by individuals who have been unknowingly recruited as money rules. *Journal of Money Laundering Control*, *24*(1), 201-212. https://doi.org/10.1108/JMLC-05-2020-0053

Esoimeme, E.E. (2018). The money laundering risks and vulnerabilities associated with MMM Nigeria. *Journal of Money Laundering Control*, *21*(1), 112-119. https://doi.org/10.1108/JMLC-01-2017-0002

Feinstein, B.D., & Werbach, K. (2021). The impact of cryptocurrency regulation on trading markets. *Journal of Financial Regulation*, *7*(1), 48-99. https://doi.org/10.1093/jfr/fjab003

Felix, T.H., & von Eije, H. (2019). Underpricing in the cryptocurrency world: Evidence from initial coin offerings. *Managerial Finance*, *45*(4), 563-578. https://doi.org/10.1108/MF-06-2018-0281

Fletcher, E., Larkin, C., & Corbet, S. (2021). Countering money laundering and terrorist financing: A case for bitcoin regulation. *Research in International Business and Finance*, *56*. https://doi.org/10.1016/j.ribaf.2021.101387

FTC (Federal Trade Commission). (2021). Cryptocurrency buzz drives record investment scam losses. *Consumer Protection: Data Spotlight*. Retrieved from https://www.ftc.gov

Gandal, N., Hamrick, J.T., Moore, T., & Oberman, T. (2018). Price manipulation in the bitcoin ecosystem. *Journal of Monetary Economics*, *95*, 86-96. https://doi.org/10.1016/j.jmoneco.2017.12.004

Gandhi, S., & Shabaz, M. (2019). Evichain: Evaluating and scrutinizing crime using block chain. *International Journal of Recent Technology and Engineering*, *8*(3), 3992-3994. https://doi.org/10.35940/ijrte.C5254.098319

Gaur, A., & Kumar, M. (2018). A systematic approach to conducting review studies: An assessment of content analysis in 25 years of IB research. *Journal of World Business*, *53*(2), 280-289. Retrieved from https://ssrn.com/abstract=3069837

Gavrilin, Y.V., Pavlichenko, N.V., & Vasilyeva, M.A. (2019). The remote approach of distribution of objects withdrawn from circulation: means, legislation issues, solutions. In A.G. Kravets (Ed.), *Big Data-driven World: Legislation Issues and Control Technologies* (pp. 85-93). Cham: Springer. https://doi.org/10.1007/978-3-030-01358-5_8

Goforth, C.R. (2021). Regulation of crypto: Who is the securities and exchange commission protecting? *American Business Law Journal*, *58*(3), 643-705. https://doi.org/10.1111/ablj.12192

Gopalan, S.H., Suba, S.A., Ashmithashree, C., Gayathri, A., & Andrews, J.V. (2019). Digital forensics using blockchain. *International Journal of Recent Technology and Engineering*, *8*(11), 182-184. https://doi.org/10.35940/ijrte.B1030.0982S1119

Hendrickson, J.R., & Luther, W.J. (2022). Cash, crime, and cryptocurrencies. *Quarterly Review of Economics and Finance*, *85*, 200-207. https://doi.org/10.1016/j.qref.2021.01.004

Hiebl, M.R.W. (2021). Sample selection in systematic literature reviews of management research. *Organizational Research Methods*. https://doi.org/10.1177/1094428120986851

Huang, D.Y., Dharmdasani, H., Meiklejohn, S., Dave, V., Grier, C., McCoy, D., & Levchenko, K. (2014). *Botcoin: Monetizing Stolen Cycles* (pp. 1-16). Retrieved from https://scholar.google.com

Hughes, A., Park, A., Kietzmann, J., & Archer-Brown, C. (2019). Beyond bitcoin: What blockchain and distributed ledger technologies mean for firms. *Business Horizons*, *62*(3), 273-281. https://doi.org/10.1016/j.bushor.2019.01.002

Irwin, A.S.M., & Dawson, C. (2019). Following the cyber money trail: Global challenges when investigating ransomware attacks and how regulation can help. *Journal of Money Laundering Control*, *22*(1), 110-131. https://doi.org/10.1108/JMLC-08-2017-0041

Jesson, J.K., Matheson, L., & Lacey, F.M. (2011). *Doing Your Literature Review. Traditional and Systematic Techniques*. London: Sage.

Karapapas, C., Pittaras, I., Fotiou, N., & Polyzos, G.C. (2020). *Ransomware as a service using smart contracts and IPFS*. Paper presented at the IEEE

International Conference on Blockchain and Cryptocurrency, ICBC 2020. https://doi.org/10.1109/ICBC48266.2020.9169451

Kirillova, E.A., Pavlyuk, A.V., Mikhaylova, I.A., Zulfugarzade, T., & Zenin, S.S. (2018). Bitcoin, lifecoin, namecoin: The legal nature of virtual currency. *Journal of Advanced Research in Law and Economics*, *9*(1), 119-126. https://doi.org/10.14505/jarle.v9.1(31).16

Kokina, J., Mancha, R., & Pachamanova, D. (2017). Blockchain: emergent industry adoption and implications for accounting. *Journal of Emerging Technologies in Accounting*, *14*(2), 91-100. https://doi.org/10.2308/jeta-51911

Konoth, R.K., Vineti, E., Moonsamy, V., Lindorfer, M., Kruegel, C., Bos, H., & Vigna, G. (2018). *Minesweeper: An in-depth look into drive-by cryptocurrency mining and its defense*. Paper presented at the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 1714-1730). https://doi.org/10.1145/3243734.3243858

Kutera, M. (2016). *Nadużycia finansowe. Wykrywanie i zapobieganie*. Warszawa: Difin S.A.

Lee, S., Meslmani, N.E., & Switzer, L.N. (2020). Pricing efficiency and arbitrage in the bitcoin spot and futures markets. *Research in International Business and Finance*, *53*. https://doi.org/10.1016/j.ribaf.2020.101200

Levin, R.B., O'Brien, A.A., & Zuberi, M.M. (2015). Real regulation of virtual currencies. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (pp. 327-360). https://doi.org/10.1016/B978-0-12-802117-0.00017-5

Liberati, A., Altman, D.G., Tetzlaff, J., Mulrow, C., Gøtzsche, P.C., Ioannidis, J.P., … Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. *Journal of Clinical Epidemiology*, *62*(10), 1-34. https://doi.org/10.1136/bmj.b2700

Lin, Y., Wu, P., Hsu, C., Tu, I., & Liao, S. (2019). *An evaluation of bitcoin address classification based on transaction history summarization*. Paper presented at the ICBC 2019 - IEEE International Conference on Blockchain and Cryptocurrency.https://doi.org/10.1109/BLOC.2019.8751410

Lorenz, J., Silva, M.I., Aparício, D., Ascensão, J.T., & Bizarro, P. (2020). *Machine learning methods to detect money laundering in the bitcoin blockchain in the presence of label scarcity*. Paper presented at the ICAIF 2020 - 1st ACM International Conference on AI in Finance. https://doi.org/10.1145/3383455.3422549

Low, K.F.K., & Teo, E. (2018). Legal risks of owning cryptocurrencies. *Handbook of Blockchain, Digital Finance, and Inclusion*: *Cryptocurrency, FinTech, InsurTech, and Regulation* (pp. 225-247). https://doi.org/10.1016/B978-0-12-810441-5.00010-5

Lu, Y. (2019). The blockchain: State-of-the-art and research challenges. *Journal of Industrial Information Integration*, *15*, 80-90. https://doi.org/10.1016/j.jii.2019.04.002

Lui, A., & Ryder, N. (2021). *FinTech, Artificial Intelligence and the Law: Regulation and Crime Prevention.* London: Routledge. https://doi.org/10.4324/9781003020998

Morgan, P.J. (2022). Assessing the risks associated with green digital finance and policies for coping with them. In F. Taghizadeh-Hesary & S. Hyun (Eds.), *Green Digital Finance and Sustainable Development Goals* (pp. 51-68). Cham: Springer. https://doi.org/10.1007/978-981-19-2662-4_3

Morin, A., Vasek, M., & Moore, T. (2021). *Detecting text reuse in cryptocurrency whitepapers*. Paper presented at the IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2021. https://doi.org/10.1109/ICBC51069.2021.9461147

Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., … Moher, D. (2021). *The PRISMA 2020 Statement: an Updated Guideline for Reporting Systematic Reviews*. https://doi.org/10.1136/bmj.n71

Parveen, R., & Alajmi, A. (2019). An overview of bitcoin's legal and technical challenges. *Journal of Legal, Ethical and Regulatory Issues*, *22*. Retrieved from https://www.abacademies.org

Patel, R., Migliavacca, M., & Oriani, M.E. (2022). Blockchain in banking and finance: A bibliometric review. *Research in International Business and Finance*, *62*. https://doi.org/10.1016/j.ribaf.2022.101718

Phillips, R., & Wilder, H. (2020). *Tracing cryptocurrency scams: Clustering replicated advance-fee and phishing websites*. Paper presented at the IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2020. https://doi.org/10.1109/ICBC48266.2020.9169433

Pimentel, E., & Boulianne, E. (2020). Blockchain in accounting research and practice: Current trends and future opportunities. *Accounting Perspectives*, *19*(4), 325-361. http://doi.org/10.1111/1911-3838.12239

Poursafaei, F., Hamad, G.B., & Zilic, Z. (2020). *Detecting malicious Ethereum entities via application of machine learning classification*. Paper presented at the 2nd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2020, 120-127. https://doi.org/10.1109/BRAINS49436.2020.9223304

Pussegoda, K., Turner, L., Garritty, C., Mayhew, A., Skidmore, B., Stevens, … Moher, D. (2017). Systematic review adherence to methodological or reporting quality. *Systematic Reviews*, *6*(1), 131. https://doi.org/10.1186/s13643-017-0527-2

Regner, F., Schweizer, A. & Urbach, N. (2019). *NFTs in practice: non-fungible tokens as core component of a blockchain-based event ticketing application*. Paper presented at the 40th International Conference on Information Systems, ICIS 2019. Retrieved from https://www.fim-rc.de

Riley, J. (2021). The current status of cryptocurrency regulation in China and its effect around the world. *China and WTO Review*, *7*(1), 135-152. https://doi.org/10.14330/cwr.2021.7.1.06

Rivera, J.W. (2019). Potential negative effects of a cashless society: Turning citizens into criminals and other economic dangers. *Journal of Money Laundering Control*, *22*(2), 350-358. https://doi.org/10.1108/JMLC-04-2018-0035

Rognone, L., Hyde, S., & Zhang, S.S. (2020). News sentiment in the cryptocurrency market: An empirical comparison with Forex. *International Review of Financial Analysis*, *69*. https://doi.org/10.1016/j.irfa.2020.101462

Rozario, A.M., & Vasarhelyi, M.A. (2018). Auditing with smart contracts. *The International Journal of Digital Accounting Research*, *18*, 1-27. https://doi.org/10.4192/1577-8517-v18_1

Sánchez, M.A. (2022). A multi-level perspective on financial technology transitions. *Technological Forecasting and Social Change*, *181*. https://doi.org/10.1016/j.techfore.2022.121766.

Sharma, G., & Bansal, P. (2020). Partnering up: Including managers as research partners in systematic reviews. *Organizational Research Methods*. https://doi.org/10.1177/1094428120965706

Short, J.C., Sharma, P., Lumpkin, G.T., & Pearson, A.W. (2016). Oh, the places we'll go! Reviewing past, present, and future possibilities in family business research. *Family Business Review*, *29*(1), 11-16. https://doi.org/10.1177%2F0894486515622294

Schmitz, J., & Leoni, G. (2019). Accounting and auditing at the time of blockchain technology: a research agenda. *Australian Accounting Review*, *29*(2), 335-342. https://doi.org/10.1111/auar.12286

Simsek, Z., Fox B., & Heavey C. (2021). Systematicity in organizational research literature reviews: A framework and assessment. Feature topic on rigorous and impactful literature reviews. *Organizational Research Methods*. https://doi.org/10.1177/10944281211008652

Srivasthav, D.P., Maddali, L.P., & Vigneswaran, R. (2021). *Study of blockchain forensics and analytics tools*. Paper presented at the 3rd Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2021. https://doi.org/10.1109/BRAINS52497.2021.9569824

Stepanov, O., Pechegin, D., & Dolova, M. (2019). Conceptual legal viewpoints on the exercise of criminal jurisdiction in the context of digitalization. *Journal of Advanced Research in Law and Economics*, *10*(5), 1541-1560. https://doi.org/10.14505/jarle.v10.5(43).25

Stix, H. (2021). Ownership and purchase intention of crypto-assets: Survey results. *Empirica*, *48*(1), 65-99. https://doi.org/10.1007/s10663-020-09499-x

Sun, Y., Xiong, H., Yiu, S.M., & Lam, K.Y. (2019). *BitVis: An interactive visualization system for bitcoin accounts analysis*. Paper presented at the Crypto Valley Conference on Blockchain Technology, CVCBT 2019. https://doi.org/10.1109/CVCBT.2019.000-3

Teichmann, F.M.J., & Falker, M. (2021). Cryptocurrencies and financial crime: Solutions from Liechtenstein. *Journal of Money Laundering Control*, *24*(4), 775-788. https://doi.org/10.1108/JMLC-05-2020-0060

Teichmann, F.M.J., & Falker, M. (2020). Money laundering via cryptocurrencies – potential solutions from Liechtenstein. *Journal of Money Laundering Control*, *24*(1), 91-101. https://doi.org/10.1108/JMLC-04-2020-0041

Torres, C.F., Baden, M., & State, R. (2020). *Towards usable protection against honeypots*. Paper presented at the IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2020. https://doi.org/10.1109/ICBC48266.2020.9169460

Toyoda, K., Ohtsuki, T., & Mathiopoulos, P.T. (2018). *Multi-class bitcoin-enabled service identification based on transaction history summarization*. Paper presented at the International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology. https://doi.org/10.1109/Cybermatics_2018.2018.00208

Trozze, A., Kamps, J., Akartuna, E.A., Hetzel, F.J., Kleinberg, B., Davies T., & Johnson, S.D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, *11*(1). https://doi.org/10.1186/s40163-021-00163-8

Turner, A.B., McCombie, S., & Uhlmann, A.J. (2019). A target-centric intelligence approach to WannaCry 2.0. *Journal of Money Laundering Control*, *22*(4), 646-665. https://doi.org/10.1108/JMLC-01-2019-0005

van Wegberg, R., Oerlemans, J., & van Deventer, O. (2018). Bitcoin money laundering: Mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, *25*(2), 419-435. https://doi.org/10.1108/JFC-11-2016-0067

Vasek, M., Bonneau, J., Castellucci, R., Keith, C., & Moore, T. (2016). The Bitcoin brain drain: examining the use and abuse of Bitcoin brain wallets. In: J. Grossklags & B. Preneel (Eds.), *Financial Cryptography and Data Security* (pp. 609-618). London: Springer.

Vasek, M., & Moore, T. (2015). There's no free lunch, even using Bitcoin: tracking the popularity and profits of virtual currency scams. In: R. Böhme & T. Okamoto (Eds.), *Financial Cryptography and Data Security* (pp. 44-61). London: Springer. https://doi.org/10.1007/978-3-662-47854-7_4

Vassar, M., Yerokhin, V., Sinnett, P.M., Weiher, M., Muckelrath, H., Carr, B., … Cook, G. (2017). Database selection in systematic reviews: An insight through clinical neurology. *Health Information and Libraries Journal*, *34*(2), 156-164. https://doi.org/10.1111/hir.12176

Venezuela's crypto-currency: Salvation or scam? (2018). *Economist* (United Kingdom), *414*(9080).

Wang, H., He, D., Liu, Z., & Guo, R. (2020). Blockchain-based anonymous reporting scheme with anonymous rewarding. *IEEE Transactions on Engineering Management*, *67*(4), 1514-1524. https://doi.org/10.1109/TEM.2019.2909529

Wang, L., Cheng, H., Zheng, Z., Yang, A., & Zhu, X. (2021). Ponzi scheme detection via oversampling-based long short-term memory for smart contracts. *Knowledge-Based Systems*, *228*. https://doi.org/10.1016/j.knosys.2021.107312

Wang, Y., Li, F., Hu, J., & Zhuang, D. (2018). *K-means algorithm for recognizing fraud users on a bitcoin exchange platform*. Paper presented at the International Conference on Electronic Business, ICEB 2018. Retrieved from http://iceb.johogo.com

Williamson, S. (2018). Is bitcoin a waste of resources? *Federal Reserve Bank of St.Louis Review*, *100*(2), 107-115. https://doi.org/10.20955/R.2018.107-15

Wronka, C. (2022). Anti-money laundering regimes: A comparison between Germany, Switzerland and the UK with a focus on the crypto business. *Journal of Money Laundering Control*, *25*(3), 656-670. https://doi.org/10.1108/JMLC-06-2021-0060

Wronka, C. (2022). Money laundering through cryptocurrencies - analysis of the phenomenon and appropriate prevention measures. *Journal of Money Laundering Control*, *25*(1), 79-94. https://doi.org/10.1108/JMLC-02-2021-0017

Zekos, G.I. (2019). *Finance Crimes: Insider Trading and Money Laundering*. New York: Nova Science Publishers. https://doi.org/10.0.204.81/CJZR6968

Zhang, Y., Kang, S., Dai, W., Chen, S., & Zhu, J. (2021). *Code will speak: Early detection of Ponzi smart contracts on Ethereum*. Paper presented at the 2021 IEEE International Conference on Services Computing, SCC 2021, 301-308. https://doi.org/10.1109/SCC53864.2021.00043

Abstrakt

CEL: *Celem głównym niniejszego opracowania jest identyfikacja aktualnego zakresu badań dotyczących kryptowalut jako przedmiotu nadużyć finansowych. Szczegółowe pytania badawcze odnosiły się do prezentacji najważniejszych kierunków tematycznych prowadzonych badań oraz zdefiniowania potencjalnych możliwości dalszej analizy tego tematu. Jedno z pytań wiązało się również z identyfikacją najbardziej popularnych oszustw przeprowadzanych z użyciem kryptowalut.* ***METODYKA:*** *Artykuł opiera się na systematycznym przeglądzie literatury (SLR) przeprowadzonym dla 57 publikacji dostępnych w bazie Scopus. Dokonano bibliometrycznej oraz opisowej analizy wybranych pozycji literatury przedmiotu. Następnie wydzielono główne klastry tematyczne i dokonano pogłębionej analizy ich treści.* ***WYNIKI:*** *Szczegółowa analiza bibliometryczna i opisowa pokazała, że tematyka kryptowalut jako przedmiotu nadużyć finansowych jest generalnie nowym obszarem badań naukowych, choć rozwija się dość intensywnie. Relatywnie mała liczba publikacji w porównaniu z innymi podobnymi obszarami pokazuje również, że ten temat nie jest jeszcze tak mocno eksplorowany przez naukowców i można w nim rozwijać wiele różnych trendów badawczych. Ostatecznie zidentyfikowano następujące kluczowe obszary badawcze:*

rodzaje oszustw kryptowalutowych, metody wykrywania nadużyć, ryzyka związane z technologią blockchain, pranie brudnych pieniędzy oraz regulacje prawne dotyczące kryptowalut. Udało się również ustalić, że obecnie najczęściej występującym przestępstwem jest pranie pieniędzy. Zwrócono jednak uwagę, że drugim dość częstym oszustwem są piramidy finansowe oparte na schemacie Ponziego. ***IMPLIKACJE:*** *W artykule wyraźnie przedstawiono główne trendy badawcze dotyczące wykorzystania kryptowalut w działalności przestępczej. Jednocześnie podkreślono, że w porównaniu do innych obszarów badawczych niniejsza tematyka jest stosunkowo nowa. Powstaje zatem szeroka możliwość eksploracji nie tylko istniejących, ale również nie odkyrtych do tej pory nurtów badawczych. Ponadto zidentyfikowano kluczowe rodzaje oszustw w praktyce gospodarczej, co jest szczególnie istotne dla uczestników rynków finansowych. Wyraźnie wskazano bowiem, które transakcje są obarczone największym ryzykiem. Warto również zwrócić uwagę na istotną aktualność tematu, gdyż skala przestępczości z udziałem kryptowalut ostatnio gwałtownie rośnie. Opracowanie potwierdza niedostateczny zakres regulacji prawnych, które nie są w stanie odpowiednio wzmocnić bezpieczeństwa obrotu gospodarczego. Może być zatem jasnym wskazaniem dla rządów poszczególnych państw, czy też instytucji międzynarodowych do dalszych sprawnych zmian przepisów prawa.* ***ORYGINALNOŚĆ I WARTOŚĆ:*** *Naukowy wkład niniejszego opracowania jest potrójny. Po pierwsze, jest to jeden z pierwszych artykułów badawczych prezentujący wyniki systematycznego przeglądu literatury (SLR) połączonego z analizą bibliograficzną oraz pogłębioną analizą treści publikacji. Podczas pracy zastosowano również oprogramowanie VOSviewer, które umożliwiło obiektywną identyfikację głównych klastrów tematycznych opartą na occurrences and link strength of keywords ujętych w publikacjach. Po drugie, zidentyfikowano kluczowe rodzaje oszustw, które jednocześnie powodują największe straty finansowe. Wyznaczono również kierunki dalszych badań, które mają głębokie praktyczne implikacje dla uczestników rynku. Niektóre z nich dotyczą bowiem konieczności opracowywania i wdrażania nowoczesnych aplikacji komputerowych, pozwalajacych na wykrywanie szerszego zakresu pojawiających się nadużyć.*

Słowa kluczowe: *kryptowaluta, bitcoin, blockchain, nadużycia finansowe, przestępstwa gospodarcze, pranie brudnych pieniędzy, schemat Ponziego, piramida finansowa, systematyczny przegląd literatury*

Biographical note

Małgorzata Kutera is an assistant professor in the Institute of Economics, Finance and Management at the Jagiellonian University in Krakow, Poland. She is also a certified public accountant (CPA) and has many years of experience in auditing financial statements. The critical areas of her research include accounting, auditing, and corporate financial reporting. Most of the publications focus on theoretical and practical aspects of auditing financial statements, the activity of statutory auditors, the organization of the audit services market, and the methodology of verification processes. In this context, fraudulent financial reporting and the role of auditing in detecting such crimes are of particular importance. Other scientific interests include the financial reporting system, creative accounting, and issues related to the tax optimization of enterprises from national and international perspectives.

Conflicts of interest

The author declares no conflict of interest.

Citation (APA Style)

Kutera, M. (2022). Cryptocurrencies as a subject of financial fraud. *Journal of Entrepreneurship, Management, and Innovation*, *18*(4), 45-77. https://doi.org/10.7341/20221842