Digital Finance (2025) 7:815–851
https://doi.org/10.1007/s42521-025-00148-1

RESEARCH

The (mis)use of cryptocurrencies by criminal organizations: a systematic literature review

Gioia Arnone[1] · **Giovanni Scire'**[1] · **Enzo Bivona**[1]

Received: 31 March 2025 / Accepted: 18 June 2025 / Published online: 18 October 2025

Abstract

This study explores the intersection between cryptocurrencies and criminal organizations through a systematic literature review. By examining peer-reviewed academic publications, the research identifies the mechanisms by which criminal groups leverage digital currencies for illicit activities such as money laundering, fraud, and extortion. A structured PRISMA-based methodology was adopted, employing well-defined inclusion, and exclusion criteria to ensure transparency and replicability. The study reveals critical trends in the misuse of cryptocurrencies, the technological challenges faced by regulators, and the limitations of current enforcement frameworks. The originality of this research lies in synthesizing existing academic insights while identifying key gaps in the literature. The findings highlight the urgent need for tailored regulatory responses and greater cross-border cooperation, contributing to both academic understanding and policymaking. The practical implications include recommendations for policy adaptation and future research pathways to mitigate cryptocurrency-enabled criminal behavior.

Keywords Crypto-enabled crimes · Illicit financial flows · Decentralized finance risks · Crypto-regulatory challenges

JEL Classification K42 · G28 · E42 · O33

✉ Gioia Arnone
gioia.arnone@unipa.it

Giovanni Scire'
giovanni.scire01@unipa.it

Enzo Bivona
enzo.bivona@unipa.it

[1] University of Palermo, Palermo, Italy

1 Introduction

The rapid evolution of digital finance has positioned cryptocurrencies as a disruptive force in the global economy. Built on decentralized blockchain technology, the digital assets offer innovative solutions for financial transactions, governance, and value exchange, challenging traditional financial institutions, and regulatory frameworks. As financial markets become increasingly data-driven and interconnected, cryptocurrencies contribute to a broader transition toward decentralized finance (DeFi), raising new questions about economic models, risk management, and regulatory oversight. Cryptocurrencies are a form of digital or virtual currency that uses cryptography for security and operates independently of a central bank (Belke & Beretta, 2020; Cunha et al., 2021). Although several other digital currencies had been developed prior to it, the advent of Bitcoin in 2009 significantly popularized the concept of cryptocurrency (Panda et al., 2023). Since then, numerous cryptocurrencies have emulated either the original source code or adapted the same, implementing their own blockchain technology and varying levels of decentralization and privacy (Guarino et al., 2022; Kirli et al., 2022). However, while cryptocurrencies provide efficiency, transparency, and financial inclusion, their pseudo-anonymous nature and decentralized architecture have also attracted criminal organizations. The anonymity-enhancing features of certain cryptocurrencies facilitate illicit activities such as money laundering, ransomware attacks, and financing of illicit markets, raising concerns among regulators and law enforcement agencies (Foley et al., 2019). As financial innovation continues to blur the lines between legitimate and illicit use, balancing technological advancement with effective regulation remains a pressing challenge in the evolving crypto ecosystem.

The cryptocurrencies can be classified based on their structure and governance into different types. One category includes pure cryptocurrency projects, which operate independently of any legal entity and evolve freely within the jurisdictions in which they exist (Allen et al., 2020). Another category consists of tokenized securities, which represent company shares issued using blockchain technology instead of traditional record-keeping methods. Similar to stocks or other securities, these tokens may signify equity or debt in a company and provide holders with rights to profits or other associated benefits. Additionally, while some cryptocurrency projects function without legal entities, certain organizations exist not to directly manage a cryptocurrency network but to support the development or application of blockchain-based assets (Ghosh et al., 2020; Liu et al., 2021; Wu et al., 2020).

Cryptocurrencies continue to gain considerable popularity worldwide, despite their initial purpose of facilitating faster and cheaper transactions than traditional payment systems (Hossain, 2021). However, their lack of consumer protections has led to their use in illegal activities (Trozze et al., 2022). Their inherent features have facilitated criminal operations such as money laundering, fraud, and extortion, which are frequently documented in the literature (Giudici et al., 2020; Hairudin et al., 2022; Kethineni & Cao, 2020). Moreover, the distinctive and

unprecedented characteristics of cryptocurrencies have expanded their applications beyond fast, private, and secure digital payments, thereby further increasing their appeal to criminal organizations (Feinstein & Werbach, 2021). These illicit ecosystems have given rise to diverse (mis)use scenarios, introducing complex financial and technological investigative challenges, as criminal organizations leverage cryptocurrencies for a wide range of unlawful activities.

The cryptocurrency ecosystem has undergone significant expansion and diversification over the past decade, inviting various criminal organizations to take advantage of its evolving services. This section offers an overview of cryptocurrency, explaining its nature and functionality. It also examines how criminal organizations can utilize cryptocurrency and the ways in which it may be (mis)used for illicit activities (Ikegwu, 2023; Marzo et al., 2022; Palmié et al., 2020; Wątorek et al., 2020; Wronka, 2023; Wu et al., 2020).

Cryptocurrency is a digital or virtual form of money designed to function as a decentralized medium of exchange. This means that it uses cryptography for security and operates on a peer-to-peer basis to manage transactions inside a blockchain or a public ledger implementation. The number of verified cryptocurrency users is currently estimated to be between 101 million and 200 million, with the number of active cryptocurrency users possibly being even higher. While the exact number of active independent cryptocurrencies is often debated, studies agree that there exist more than 1000 cryptocurrencies in the market, with Bitcoin, Ethereum, and Tether being some of the most used. The value of cryptocurrencies is measured similarly to that of equities, thus resembling more commodities than traditional currency. The total market capitalization of all cryptocurrencies is estimated to be around $300 billion (Bublyk et al., 2023; Momtaz, 2021). The increasing adoption of cryptocurrencies has not only revolutionized financial transactions but has also facilitated illicit activities, making them a preferred tool for criminal organizations worldwide. Darknet marketplaces such as Silk Road between 2011 and 2013) and its successors AlphaBay and Hansa in 2017 enabled the anonymous sale of drugs, weapons, and counterfeit goods, with Bitcoin (BTC) serving as the primary medium of exchange before law enforcement agencies intervened (Andrei & Veltri, 2025; Dayoub et al., 2024; Hemdani, 2025; Nali et al., 2025) Similarly, ransomware attacks have escalated with cryptocurrencies playing a central role in extortion schemes, as demonstrated by the 2021 Colonial Pipeline attack (Cong et al., 2025; Longa, 2025), where the DarkSide hacking group demanded ransom in BTC, and the Ryuk ransomware attacks, which extorted millions in Bitcoin and Monero (XMR) from global institutions (Bhardwaj, 2024; Cohen et al., 2025). Furthermore, money laundering through crypto mixers and tumblers has become a widespread practice among criminal networks. The U.S. Treasury's sanctions against Tornado Cash in 2022 (Fylaktou & Savvides, 2025; Scharfman, 2024) and Europol's shutdown of ChipMixer in 2023 (Liu & Dong, 2025; Nicholls et al., 2024) underscore the growing role of these tools in concealing illicit transactions, including funds linked to the North Korean Lazarus Group (Hamilton & Leuprecht, 2024).

Beyond financial crimes, the terrorist organizations have increasingly leveraged cryptocurrencies for fundraising. Investigations into Hamas in 2023 and ISIS between 2015 and 2017 revealed their use of Bitcoin, Ethereum, and Tether (USDT)

for operational funding, prompting regulatory crackdowns (Akcinaroglu & Shi, 2025; Chitsungo, 2024).

Fraudulent schemes, such as the OneCoin Ponzi scheme between 2014 and 2017 (Agarwal et al., 2024a; Smith, 2024), which defrauded investors of $4 billion, and BitConnect between 2016 and 2018 (Chen et al., 2025), a pyramid scheme causing losses of $2.4 billion, further illustrate how cryptocurrencies have been exploited for illicit financial gain. Drug cartels, including the Sinaloa and Jalisco New Generation Cartels (CJNG), have reportedly used Bitcoin ATMs to launder money, while Chinese fentanyl suppliers accept cryptocurrency payments to facilitate the global synthetic drug trade (Cusumano, 2024; Windsor, 2024). Moreover, Venezuela's controversial launch of the Petro cryptocurrency has been cited as an attempt to circumvent U.S. economic sanctions (Ibrahim et al., 2024; Mumford et al., 2024).

The relationship between cryptocurrencies and criminal activities is a multifaceted one (Kutera, 2022; Leuprecht et al., 2023). One of the most noteworthy issues is their decentralized nature. This characteristic makes cryptocurrencies attractive for criminal organizations, as they can operate without a central authority overseeing their behaviors. This is further supported by their anonymity, which is the result of the cryptocurrency itself. All cryptocurrencies use a distributed ledger as the "backbone" of their system, which makes it economically very difficult to reverse or otherwise modify transactions, further supported by their anonymity, which is the result of the cryptocurrency itself (Ahmed & Alabi, 2024). All cryptocurrencies use a distributed ledger as the "backbone" of their system, which makes it economically very difficult to reverse or otherwise modify transactions. Users can have multiple addresses, effectively hiding their movements. This is especially powerful as multinational organizations can switch between separate entities within their structure to make breaches harder to track. The combination of decentralization and anonymity makes cryptocurrencies highly resistant to tracking and oversight. A number of recent reports provide additional insight into this. To better understand this complex issue, it is evident that detailed research is warranted and timely (Ghosh et al., 2020; Krishnan, 2020; Zarrin et al., 2021). In recent years, the symbolic boundary between cryptocurrency and crime has narrowed in the public domain (Buil-Gil & Saldaña-Taboada, 2022; Cherniei et al., 2021; Courtois et al., 2021; Dulisse et al., 2024; Dupuis et al., 2023; Maurushat & Halpin, 2022; Steinmetz et al., 2021; Teichmann & Falker, 2021).

Separately, these elements have always existed, but they have increasingly become intertwined. Cryptocurrencies are often celebrated for their innovation, enabling wholly new forms of transactions, online payment, and finance (Allen et al., 2022; Faccia et al., 2020; Martino, 2021; Mikhaylov, 2023).

The decentralized ledger technology of blockchain decreases or eliminates the necessity for mediators in financial transfers and weakens government control over resources and distribution. Peer-to-peer networking additionally increases the opportunity for anonymity within transactions, thereby empowering criminal organizations to operate in untaxed, extorted, trafficked, laundered, or smuggled activities (Choi et al., 2020; Hou et al., 2020; Shan et al., 2021).

While cryptocurrencies have been celebrated for enabling easy, cost-effective transactions between potential buyers and sellers, their particular benefits to

criminals and illicit actors have received less scrutiny (Alfieri, 2022; Leuprecht et al., 2023; Wronka, 2023). Cryptocurrency's easy pseudonymity increases a sense of security and confidentiality for the transactor when operating, which is appealing to those with a criminal disposition. Therefore, it is essential to comprehend the various ways in which criminal organizations (mis)use cryptocurrencies to operate illicit activities, identify the various typologies produced, trying to address the implications for policy and law enforcement (Cherniei et al., 2021; Leuprecht et al., 2023; Steinmetz et al., 2021).

Given the growing interest in the relation between cryptocurrency and criminal organizations and the need to consolidate research in the field, this systematic review aimed to provide a specific structure by adding comprehensive insight with a broad analysis through selecting, analyzing, and synthesizing primary studies (Luong, 2023; Silva & Mira da Silva, 2022). In the context of cryptocurrency and crime, tax evasion, money laundering, drug trafficking, terrorism, dark web, and cybercrime have been better studied, but the (mis)uses for criminal organizations have been inadequately assessed (Gonzálvez-Gallego & Pérez-Cárceles, 2021; Trozze et al., 2022; Wang & Zhu, 2021).

To date, no methodological literature analysis has been carried out with the aim of understanding if and how academic literature relating to cryptocurrency refer to crime and, in particular, to the different types of criminal organizations evoked as potential users. Thus, the present systematic review attempts to enrich our knowledge on (mis)uses of these technologies by systematically reviewing, analyzing, and synthesizing empirical research studies related to cryptocurrency and crime. In particular, the specific focus of the systematic review concentrates on examining the ways in which criminal organizations (mis)use cryptocurrencies when engaged in illegal activities or in the commission of illicit criminal operations, which compose a puzzle of a broader financial cyber fraud ecosystem (Bartoletti et al., 2021; Kutera, 2022; Nicholls et al., 2021; Radanliev, 2024; Trozze et al., 2022; Wronka, 2023).

Therefore, the present work aims to comprehensively review how criminal organizations (mis)use cryptocurrencies. With growing interest in the link between cryptocurrency and crime, this systematic review provides a structured analysis by selecting, analyzing, and synthesizing primary studies (Luong, 2023; Silva & Mira da Silva, 2022). While money laundering, drug trafficking, terrorism, the dark web, and cybercrime are well-studied, the (mis)use of cryptocurrencies by criminal organizations is under-researched (Gonzálvez-Gallego & Pérez-Cárceles, 2021; Trozze et al., 2022; Wang & Zhu, 2021). Thus, the present review aims to address this gap by examining studies on cryptocurrency and crime, focusing on how criminal organizations use cryptocurrencies for illegal activities, contributing to a more comprehensive understanding of the context of financial cyber fraud (Bartoletti et al., 2021; Kutera, 2022; Nicholls et al., 2021; Radanliev, 2024; Trozze et al., 2022; Wronka, 2023). The paper's novelty lies in the interest of particular interest or may be used to improve the future development of national and international intergovernmental organizations with experience in cryptocurrency-related matters, as these organizations continue to develop extensive regulatory reporting recommendations for institutions and stakeholders (Badawi & Jourdan, 2020; Bahamazava & Nanda, 2022;

Bartoletti et al., 2021; Ferdous et al., 2021; Nyhus et al., 2024; Steinmetz et al., 2021).

1.1 Research gap

The increasing use of cryptocurrencies by criminal organizations presents a multidimensional challenge for policymakers, law enforcement agencies, and financial regulators. This study synthesizes existing academic literature to identify how and why these technologies are exploited for illicit purposes, including money laundering, fraud, extortion, and financing of criminal operations. While the academic literature has grown significantly around cryptocurrencies and blockchain technology, relatively few studies have systematically explored the intersection between cryptocurrencies and organized criminal behavior through a structured methodological lens. Existing work tends to be either legal-descriptive, focusing on regulatory responses, or technology-centered, emphasizing the technical characteristics of blockchain and anonymity (Giudici et al., 2020; Hairudin et al., 2022). However, a comprehensive synthesis that bridges criminological, financial, and legal perspectives remains largely absent. Additionally, few studies adopt a transparent, replicable methodology to map the evolving patterns of crypto-enabled illicit activities. This study addresses these gaps by conducting a systematic literature review, offering an interdisciplinary synthesis that captures not only the mechanisms of criminal exploitation of cryptocurrencies but also the implications for enforcement, regulation, and policy. Based on the literature gaps and the increasing policy relevance of cryptocurrency-enabled crime, this study pursues the research objective of identifying, classifying, and interpreting the ways in which cryptocurrencies are used by criminal organizations and to evaluate the institutional and regulatory responses found in the academic literature. To guide the analysis, we propose the following working hypothesis: the inherent technical features of cryptocurrencies—such as decentralization, anonymity, and global reach—make them especially attractive to criminal organizations, resulting in persistent regulatory challenges across jurisdictions. This hypothesis is examined through a systematic literature review and validated by synthesizing thematic patterns found in peer-reviewed academic sources.

Our findings suggest that the combination of pseudo-anonymity, lack of consumer protection, and cross-border functionality make cryptocurrencies particularly attractive to criminal actors. The originality of this paper lies in its interdisciplinary and methodologically rigorous approach to mapping the evolving criminal use of cryptocurrencies. By identifying patterns, knowledge gaps, and enforcement challenges, the study contributes to a more integrated academic and policy dialog on digital financial crime.

The policy implications of our findings are significant. We highlight the need for greater international regulatory coordination, improved tools for tracking illicit transactions, and the development of crypto-specific compliance and enforcement mechanisms. These insights aim to support decision-makers in crafting more effective and adaptable frameworks for combating crypto-related crime.

The sections of this paper are organized as follows: after a brief introduction to the topic of cryptocurrencies and crime, the second section of this article illustrates the theoretical foundations of the relationship between cryptocurrencies and criminal activities. Section 3 details the research methodology, including search strategy, inclusion/exclusion criteria, and coding process. Section 4 presents the results, organized around major themes and patterns identified in the literature. Section 5 discusses practical implications, concrete examples, and policy recommendations. Section 6 concludes by summarizing findings and offering suggestions for future research.

2 Description of the procedure: presentation of the 'Systematic Literature Analysis' method

The present study employs the systematic literature review approach (Collins et al., 2021) due to the fact that a significant portion of the extant knowledge regarding cryptocurrency (mis)use by criminal organizations is dispersed across various fields of inquiry and institutional settings.

The process is frequently referred to as a "systematic review" or "research overview" (Koropogui et al., 2025; Lim, 2025). An SLR seeks to take into account and assess the state of theories, research, and methodology on a certain subject. It typically always follows a predetermined framework that is similarly described in numerous publications, employing a six-step summary of multiple approach descriptions: (i) Defining the research question to define the time horizon, relevance, and goal of the SLR; (ii) Identifying the necessary features of sources, such as the creation of inclusion and exclusion criteria; (iii) Finding a selection of potentially relevant literature to verify the search strategy and keywords to use later; (iv) Choosing the literature pertinent to the synthesis, including inclusion and exclusion criteria; (v) Executing the synthesis; (vi) Processing the findings (Kraus et al., 2022; Rad et al., 2022; Sauer & Seuring, 2023).

To identify and interpret conceptual and methodological problems, SLR is an effective tool (Boell & Cecez-Kecmanovic,2015; Crossan & Apaydin, 2010; Sarmento & Simões, 2018). It can also inform the development of theory and suggest significant topics for further study (Hulland et al., 2018; Kohtamäki et al., 2018), emphasizing the need for empirical research to methodically identify and comprehend certain research topics, their gaps, and their potential for further study. By integrating research from multiple disciplines, a comprehensive understanding of the existing body of knowledge can be achieved, highlighting the interrelationships among distinct conceptions, study areas, and broader literature fields (Bonkile et al., 2018). The design stage of the literature review approach involved creating inclusion/exclusion criteria for the chosen published materials (Hulland et al., 2018; Kohtamäki et al., 2018). The study only looks at peer-reviewed scientific papers published in esteemed publications.

As a relatively new subject, cryptocurrencies have not attracted extensive research attention and the scientific knowledge about their potential use by criminals is dispersed in a variety of documents that are useful for this paper and come

from a broad operational and specific literature (Cherniei et al., 2021; Kutera, 2022; Teichmann & Falker, 2021; Wu et al., 2020). Moreover, the rapid growth of cryptocurrencies suggests that this particular form of payment could impact crime prevention and money laundering operations, substantially deepening its practical significance in such contexts (Siqueira et al., 2020). Therefore, the development of a review designed to collect and test practical advice supplied in a broad literature on these points appears particularly useful. Third, the completion of a research review allows the classification of whether future research can improve on what has already been done and whether the results of such studies could be used in collective decision-making processes (Akartuna et al., 2022; Dupuis & Gleason, 2021; Guidara, 2022; Wronka, 2022). Likewise, this synthesis can ascertain the existence of practical recommendations from academic institutions, validate existing policies, identify potential future research areas, and assess the utility of instruments developed within the scientific community for investigative purposes. These characteristics are particularly useful for this study when its objective is assessed: to systematically review and analyze the existing literature with the aim of summarizing the information available on cryptocurrency use in the context of organized crime (Dupuis & Gleason, 2021; Hossain, 2023; Trozze et al., 2022).

3 Selection of a suitable search method

To test the proposed hypothesis and to fulfill its stated objective, this study conducts a systematic literature review (SLR) based on the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework to ensure replicability, transparency, and comprehensiveness. The review process began with a well-defined search protocol using the Scopus and Web of Science databases, chosen for their extensive coverage of high-quality, peer-reviewed literature. The search strings combined selected keywords, reported in detail later in this paragraph, to capture the intersection between digital financial technologies and criminal activities.

The inclusion criteria required that papers be peer-reviewed, written in English, and directly relevant to both cryptocurrency and criminal activity. The exclusion criteria eliminated duplicates, conceptual papers not linked to empirical data or criminological implications, and non-scholarly sources. A three-step process was applied: (1) initial search and de-duplication, (2) screening by title and abstract, and (3) full-text review and thematic coding.

This structured search and filtering process adheres to the rigor of evidence-based reviews. Compared to traditional narrative reviews or expert-opinion syntheses, this method reduces bias and improves reproducibility. Unlike machine-learning-based content mining or meta-analyses requiring statistical aggregation, the SLR allows a broader thematic capture of both qualitative and interdisciplinary insights. Its limitations include potential omission of gray literature and studies not indexed in the chosen databases, which may slightly narrow the scope. However, the structured PRISMA methodology ensures methodological clarity and offers a robust foundation for both future replication and expansion.

More in details, to conduct the present systematic literature review on the use of cryptocurrency by criminal organizations, a comprehensive search strategy was employed. The search was conducted via the Scopus database search engines (Barhate & Dirani, 2022; Cartwright et al., 2021; Hendricks & Mwapwele, 2024).

For the literature search, the search strings primarily include the themes of '*Cryptocurrency*' AND '*Crime*', '*Cryptocurrency*' AND '*Criminal Organizations*', '*Cryptocurrency*' AND '*Terrorist Financing*', and '*Cryptocurrency*' AND '*Money Laundering*' with the aim of capturing a wide range of academic studies relevant to the research topic. The keywords such as 'cryptocurrency', 'virtual currency', and 'digital currency' along with their plural forms, were combined with terms *'crime'* and *'criminal organization'* to optimize the search results. The methodological framework draws upon prior systematic review approaches (Badawi & Jourdan, 2020; Trozze et al., 2023), ensuring a rigorous selection of studies for analysis.

To bring together the results of the literature research, the inclusion and exclusion criteria were applied to ensure the relevance and quality of the selected articles. Subsequently, to reveal the current state of the art and research directions within a field, setting a recent timeframe was recommended (Mohamed Shaffril et al., 2021). Thus, studies published between 2020 and 2024 in peer-reviewed academic journals, written in English and presenting empirical findings were included.

More in details, the initial sample consisted of 305 articles, whose titles, abstracts, and keywords were examined for relevance to the topic as part of the SLR. In some cases, although the title and keywords appeared promising, the content of the abstract was of little relevance for our SLR. These articles were then excluded, following the approach of Kohtamäki et al. (2018), who argued that generic articles with no particular contribution to the research question should be excluded. Additional eligibility criteria were applied to ensure the inclusion of research highly relevant to the intersection of cryptocurrencies and criminal activities: exclusion criteria eliminated studies published before 2020, non-peer-reviewed articles, single case studies, unpublished theses or dissertations, and papers. After removing duplicate entries using DOI identifiers, this filtering reduced the dataset from 305 peer-reviewed articles to 245 relevant scientific papers relevant for the study remaining for further screening.

To provide an overview of the literature and develop a consolidated synthesis of information from a variety of subjects underlining the crime (mis)use of cryptocurrencies by criminal organizations (Badawi & Jourdan, 2020; Bartoletti et al., 2021; Guidara, 2022), we only reviewed English contributions.

The aim was to identify all papers investigating potential criminality, enabling an assessment of the scope of research conducted on this topic (Yang et al., 2024). To give an overview on the connection between the (mis)use of cryptocurrencies and criminal organizations, 127 papers related to the (mis)use of virtual currency were identified (Chiarini, 2020). Figure 1 illustrates the search strategy design process for articles included in this systematic literature review.

The overall amount of literature available for an SLR is limited by inclusion and exclusion criteria (Table 1). Analyzing the distribution of academic outputs across different publication formats of the 127 materials identified for the present work, it can be observed (Table 2) that the majority of the academic outputs comes from

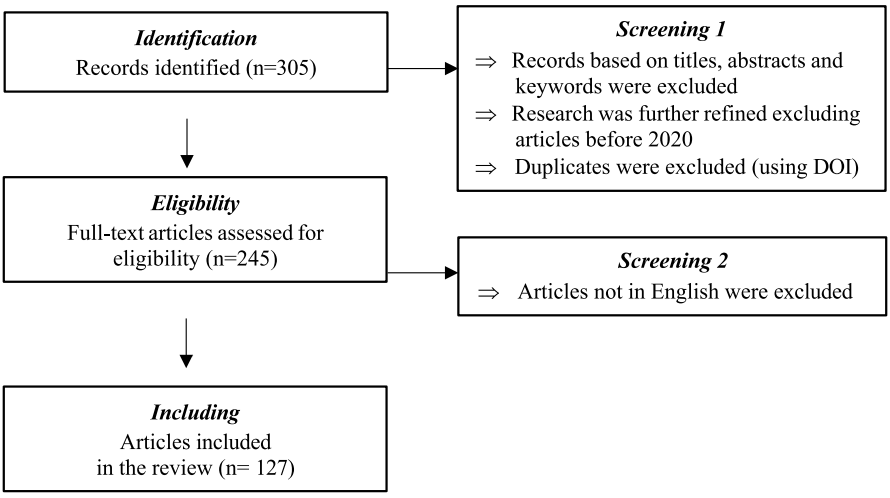

Fig. 1 PRISMA diagram for inclusion of articles. Source: The Authors

journal publications, indicating a preference on peer-reviewed journals (77 sources); a smaller number of publications are in the form of monographs, which are often used for more comprehensive studies (20 sources); while a moderate share of publications are presented at academic conferences, highlighting their role in disseminating research findings (30 sources).

Table 3 presents the most frequently cited academic journals in this systematic literature review, highlighting key sources that have contributed to research on cryptocurrencies, financial crime, and regulatory issues. These journals have published multiple articles on the subject, reflecting their relevance in the academic discourse:

Considering the objective of the research, we may classify the current investigation under the exploratory research using a qualitative technique as we wish to demonstrate the relationship between the (mis)use of cryptocurrencies and criminal organizations (Fülöp et al., 2024).

4 Results

4.1 Analyzing the (mis)use of cryptocurrencies by criminal organizations

The (mis)use of cryptocurrencies by criminal organizations is facilitated by a variety of techniques and represents a dynamic and evolving process where criminals exploit the technological aspects of cryptocurrencies (Adiyatma & Maharani, 2020; Badawi & Jourdan, 2020; Dupuis et al., 2023; Leuprecht et al., 2023; Teichmann & Falker, 2021; Trozze et al., 2023).

It has been observed that crime organizations are leveraging methods employed by legitimate users to facilitate the secure, fast, and cost-effective transfer of cryptocurrencies across international borders (Leuprecht et al., 2023; Wronka, 2022). The

Table 1 Inclusion and exclusion criteria. Source: The Authors

Criteria	Inclusion	Exclusion
Publication Year	Studies published between 2020 and 2024	Studies published before 2020
Publication Type	Peer-reviewed journal articles, conference proceedings	Non-peer-reviewed articles, unpublished theses, dissertations, single case studies
Language	English	Articles in languages other than English
Empirical Evidence	Studies presenting empirical findings	Theoretical or conceptual papers without empirical data
Topic Relevance	Articles containing 'Cryptocurrency' AND 'Crime', 'Cryptocurrency' AND 'Criminal Organizations' in the title, abstract, or keywords	Genericarticleswithnoparticular contribution to the research question
Keywords Used	'Cryptocurrency','VirtualCurrency', 'Digital Currency' combined with 'Crime' or 'Criminal Organization'	Articles that do not include relevant terms in the title, abstract, or keywords
Duplicates	Unique articles (duplicates removed using DOI identifiers)	Duplicate entries in the database (removed using DOI identifiers)
Journal Prestige	Published in reputable academic journals or conference proceedings	Studies from unrecognized sources or low-impact journals

Table 2 Distribution of academic publications by source type. Source: The Authors

Scientific Source	Number of publications
Academic Journals	77
Monographs	20
Conference Proceedings	30

Table 3 Most recurrent academic journals in the systematic literature review. Source: The Authors

Journal Name	Number of articles
Journal of Financial Crime	11
Journal of Money Laundering Control	10
IEEE Access	9
Technological Forecasting and Social Change	4
Journal of Risk and Financial Management	4
Journal of Economic Criminology	3
Journal of Criminal Justice	3
Journal of Forensic and Investigative Accounting	2
Journal of International Money and Finance	2
Journal of Business Research	2
Others	77

high volume of transactions within these networks poses significant challenges for law enforcement agencies in tracking illicit activities. The proliferation of underground banking services and other online money-laundering networks has led to the development of more anonymous financial transfer systems (Wang & Hsieh, 2024). The potential of cryptocurrencies to be (mis)used by criminal organizations is increased because the industry is encountering sophisticated new solutions and peer-to-peer cryptocurrency mixing services that obscure transactions from regular decentralized blockchain analysis of cryptocurrencies, while the rise of newly launched peer-to-peer networks is likely to play a viable role in the process of illegal activity (Wu et al., 2020)

Since its inception, money laundering has been a critical tool for concealing illicit financial activities. With the rise of new technologies and cryptocurrencies, increasingly sophisticated methods are expected to emerge, offering greater security and more advanced techniques. These developments will further complicate the detection of criminal activities that exploit traditional cryptocurrency solutions to obscure illicit monetary gains (Choi et al., 2020).

The benefits of cryptocurrencies for criminals are numerous: the transfer of drugs, weapons, and other contraband is a lucrative use case for cryptocurrencies since it enables easy transfer of illicit funds to and from offenders from any location in the world (Feinstein & Werbach, 2021). The ease with which hackers can access cryptocurrency systems around the world has created a new attack surface for cybercriminals, who can choose from a variety of attack vectors. Among

the most prominent of these undesirable side effects are ransomware attacks. Whereas money laundering can, and has been done outside the cryptocurrency ecosystem, the lack of identity verification and other regulatory oversight can make cryptocurrency money laundering less burdensome. Ultimately, beyond scams, the cryptocurrencies have been associated with nearly all categories of cybercrime, ranging from dark web services to various forms of theft and fraud. The interaction between cryptocurrency and criminal organizations is intricate, and the pseudo-anonymous nature of cryptocurrency, coupled with the absence of central oversight, has resulted in a multitude of criminal (mis)use cases. This happens directly through the use of cryptocurrencies for various illegal transactions or through secondary activities, such as mining as a means of obtaining funds. The utilization of cryptocurrency in a wide range of criminal activities, including money laundering, ransomware attacks, and internet fraud, has been documented. In order to combat these illicit practices, law enforcement agencies have been provided with a comprehensive overview of the available literature on the subject (Macfarlane, 2021; Trozze et al., 2023; Watters, 2023).

The research conducted on the (mis)use of cryptocurrency by criminal organizations is still limited in comparison to other topics of research in the field of cryptocurrency and blockchain. Among the types of roles dishonestly carried out by criminal organizations using virtual currency, there is the use of virtual currency—among the other—for money laundering, as revenue from criminal activity, for ransomware, in the dark markets (Custers et al., 2020; Faccia et al., 2020; Mugarura & Ssali, 2020; Nizovtsev et al., 2022; Patsakis et al., 2024; Wronka, 2022).

We conducted a systematic evaluation of specialist literature to accomplish this goal (Chawla & Mehta, 2023; Windari et al., 2024). Following the approach outlined by Alqudah et al. (2023), we completed the following steps to accomplish our suggested goal of conducting a systematic analysis: (i) defined the keywords for database searches; (ii) defined the query string for database searches and downloads of the necessary information; iii) chose databases that contained electronic information publications; (iv) searched the publication databases; (v) examined the search results; (vi) downloaded the publications; (vii) reviewing the retrieved publications for relevance; viii) examined the thematic content of the selected studies (Fülöp et al., 2024). Building upon previous research that has employed co-word analysis and citation mapping techniques to identify conceptual structures in the field (Meng et al., 2020; van Eck & Waltman, 2017), we performed a human-based thematic clustering of the literature (Machado et al., 2024). This qualitative classification allowed us to group the studies into seven thematic areas, representing the major forms of (mis)use of cryptocurrencies by criminal organizations. The following seven thematic clusters have been identified: (1) Cryptocurrency and Terrorist Financing, (2) Cryptocurrency and Money Laundering, (3) Cryptocurrency and Dark Web Markets, (4) Cryptocurrency and Cybercrime, (5) Cryptocurrency and Drug Trafficking, (6) Cryptocurrency and Human Trafficking, (7) Cryptocurrency and Corruption. In particular:

- ***Cluster 1: cryptocurrency and terrorist financing***

The use of cryptocurrency in the context of terrorist financing can have a pronounced effect on various regions worldwide, thereby significantly mitigating the challenges associated with conventional methods of financing terrorism. Cryptocurrency can be used without the need for authorization, and it is unregulated by any jurisdictional authority. These attributes mostly allow criminal organizations or terror operators to turn traceable money into another form, which is more widely accepted. Cryptocurrency, especially common virtual coins, displays a degree of anonymity. The majority of financial transactions conducted within the Bitcoin network are obscured by a combination of mixing, swapping, and tumbling techniques, suggesting the presence of advanced advantages over other cryptocurrencies. Notably, Bitcoin's network has been observed to feature a well-established money laundering system, particularly within underground exchanges. This system enables the conversion of Bitcoin into physical cash that is not subject to legal jurisdiction (Andrianova, 2020; Leuprecht et al., 2023; Mikhaylov et al., 2021). With the help of cryptocurrency, those criminals can raise funds for purposes such as defection, assistance in starting wars, and support in attacking territorial targets. Furthermore, the virtual currencies have facilitated the emergence of numerous merchants with clandestine and overt objectives, thereby enabling the accumulation of funds by organized dissidents engaged in supporting armed attacks. These ransoms are further encouraged to be used to help militant fighters, support their families, and provide food, necessities of life, weapons, and support for military units. This, in turn, increases the ability of those criminals to launch multiple terrorist attacks (Andrianova, 2020; Teichmann, 2022).

- ***Cluster 2: cryptocurrency and money laundering***

Money laundering is the process of concealing illegally obtained funds through various legal procedures, with the invested money subsequently being involved in legal growth (Sharif & Ghodoosi, 2022).

Malicious organizations use multiple, complex systems that provide fault tolerance. In addition, decentralized networks like cryptocurrency are ideal to be abused by malicious organizations due to their inherent anonymity, lack of a central authority, and fast transactions that obscure the movement of funds. With the blockchain and the intrinsic cryptographic characteristics, Bitcoin is a good candidate for money laundering and other legal spending. Layered and staged transactions can be employed to obfuscate ownership and severely diminish the ability to trace transactions. The usage of mixed services can confuse day-to-day transactions as well, which can make the law enforcement tracing process more difficult. Other cryptocurrencies offer special anti-tracing approaches, which allows a user to hide traceability compared with Bitcoin. Also uses a special algorithm to hide transaction aspects. But all these approaches eventually open backdoors because they are not designed to support these properties, and they are offered along with additional technological mechanisms commonly employed in cryptocurrencies (Bjelajac & Bajac, 2022; Wronka, 2022).

The first layer of protection is anonymity. In an ideal cryptocurrency world, it would be difficult to make a transaction linked to an owner. The process would

include multiple wallets and diverse public keys and blockchains. The secret identities can only be established or revealed to another party with the appropriate cryptographic approval. Blockchains are, therefore, inconvenient for those attempting to transact outside of the law (Dupuis & Gleason, 2021). Money laundering using cryptocurrency is still a serious problem and a significant weakness in the design of decentralized cryptocurrencies. It weakens crime prevention, provides illegal commodities to criminals, helps circumvent data sharing practices, renders blacklist systems ineffective, and assists the use of compromised cryptocurrencies, among other issues, rendering money laundering a serious problem for operational financial systems as a whole.

Various forms of money laundering are being effectively addressed, particularly in cases where goods are sold online for legitimate cryptocurrencies, as this represents one of the few tangible links between cryptocurrency and the real world. However, anonymous cryptocurrencies remain misunderstood by dishonest traders and money launderers. This challenge is being met through a range of measures, including strengthened regulatory frameworks, a combination of legal and extralegal strategies, and intensified enforcement efforts. Despite these advancements, the issue is likely to persist as an ongoing vulnerability. Effective regulatory solutions will require ensuring that cryptocurrency exchanges can verify end users and trace transactions back to legitimate entities. Consequently, money laundering and the associated enforcement challenges represent significant weaknesses that the cryptocurrency market must address to secure its long-term viability as a trusted financial instrument (Wu et al., 2020; Zarrin et al., 2021).

- ***Cluster 3: cryptocurrency and dark web markets***

Given the prominent role of cryptocurrencies in the commercial activities of darknet marketplaces, a body of research was conducted on cryptocurrency usage for online trading of illegal goods and services in "dark web" marketplaces (Besenyő & Gulyas, 2021; Faccia et al., 2020). The transactions conducted on the dark web have been shown to involve money laundering, malfeasance, and the commercial exchange of illegal goods and services, resulting in substantial cost savings. These transactions often yield substantial profits for dealers, with 24% of transactions exceeding notable sums. A significant number of the online transaction marketplaces identified in this study are hosted in the dark web—accessible only through services such as Tor—and facilitate the exchange of Bitcoins for a range of illegal goods and services. Core to this market is the anonymity of transactions and of the clients and sellers involved (Bright et al., 2023; Chlebowicz & Buczyński, 2023). The things that attract people to trading Bitcoin, in other words, are also things that attract people to buying illicit substances. A notable development is the increase in dark web transactions between buyers and sellers on the same continent, with family members often serving as drug mules in these transactions (Akcinaroglu & Shi, 2023). Drugs, non-prescription medications, and steroids are offered in open sale in a fast-growing, well-stocked arena of commercial outlets. These substances are available in quantities significantly higher than previously documented (Bjelajac

& Bajac, 2022; Chawki, 2022; Wronka, 2022). In particular, in this world where the demand for weapons is constant (Braga et al., 2021), the nexus between cryptocurrency and weapons trafficking (Kethineni & Cao, 2020; Leonidou et al., 2023; Mademlis et al., 2023) surely make these virtual currencies the ideal bargaining chip so that many of the intermediaries could be replaced by non-human interfaces (Alfieri, 2022; Bahamazava & Nanda, 2022; Kreminskyi et al., 2021).

- ***Cluster 4: cryptocurrency and cybercrime***

The rapid rise of cryptocurrencies has profoundly impacted the criminal landscape, particularly by facilitating transactions that are difficult to trace. These digital assets have gained notoriety for their role in supporting illicit activities such as ransomware, scams, and phishing (Courtois et al., 2021; Galit et al., 2024).

Ransomware attacks, in which malware encrypts victims' data until a cryptocurrency ransom is paid, have emerged as a significant cybersecurity threat. Cryptocurrencies such as Bitcoin are preferred for their ease of transfer and anonymity, complicating enforcement efforts and enabling attackers to launder funds and evade authorities (Bjelajac & Bajac, 2022; Kaplan, 2021; Sangal et al., 2024). Moreover, the rise of "ransomware-as- a-service" platforms has democratized access to these tools, enabling even unskilled attackers to profit from cybercrime (Hossain, 2023). Scams and phishing attacks have evolved, exploiting technological advancements and leveraging cryptocurrencies to conceal financial operations. Phishing services target individuals and organizations, harvesting credentials to compromise secure systems, often leading to significant financial losses (Agarwal et al., 2024b; Greco & Greco, 2020). The interplay between vulnerabilities in cryptocurrency interfaces and user awareness renders them susceptible to spoofing and laundering techniques (Bartoletti et al., 2021; Ghazi-Tehrani & Pontell, 2021). The pandemic of Coronavirus Disease 2019 (COVID-19) gave rise to phishing scams linked to vaccination certificates, leveraging social engineering to infiltrate systems, and maximize financial gain (Jain & Gupta, 2022). These tactics have become increasingly sophisticated, targeting victims' desperation to recover data or funds (Meland et al., 2020). Ransomware attackers demand cryptocurrency payments for decryption keys, exploiting the victims' inability to trace transactions due to cryptocurrencies' decentralized and pseudonymous nature (Sokolov, 2021).

The rise of cryptocurrencies has fueled the expansion of illicit gambling markets, enabling new forms of financial crime. Cryptocurrencies provide a degree of anonymity that traditional financial institutions cannot, making them a preferred medium for unregulated online betting platforms and fraud schemes; particularly Bitcoin, have facilitated illegal sports gambling and online casinos operating outside regulatory oversight. These platforms often evade gambling laws by using in-game virtual currencies (so-called "zero-value currencies") which technically hold no legal monetary status but can be exchanged for real-world assets through secondary markets. Moreover, the integration of blockchain-based assets into gambling has contributed to the development of "skins betting", a billion-dollar industry where in-game items are wagered and monetized through third-party exchanges, frequently beyond the reach of law enforcement. In the dark web, the cryptocurrencies

are widely used in fraudulent gambling operations and Ponzi schemes, where victims are lured into investment scams promising high returns. Illicit betting rings operating via encrypted networks further complicate regulatory enforcement, as transactions remain pseudonymous. Additionally, cryptocurrency-based gambling platforms have been linked to money laundering operations, where criminal organizations exploit digital casinos to clean illicit funds (Gainsbury & Blaszczynski, 2017; Holden, 2018; Steinmetz, 2023).

Law enforcement faces hurdles in identifying perpetrators, as linking stolen funds to an exchange account is often the only way to trace them (Wang et al., 2021). Although cryptocurrencies are not inherently criminal, their misuse arises from their pseudonymity and decentralization. To this end, enhancing regulatory frameworks and strengthening cybersecurity measures are essential to mitigating cryptocurrency-related cybercrime (Agarwal et al., 2024b; Teichmann & Falker, 2021).

- ***Cluster 5: cryptocurrency and drug trafficking***

The sale of drugs is not new to humanity, with origins dating back to the government ban that led to the crackdown on alcohol consumption. Since then, networks for the sale of banned substances have developed worldwide, and the market takes place in several cities around the world. From traditional drug flows such as marijuana, powder cocaine, crack, and heroin, which are the most smuggled drugs, to newer synthetic substances, the demand for drugs increases on a daily basis and even more with the variety of paths now set, such as the use and intervention of cryptocurrencies (Shortis et al., 2020). In this emerging era of cyber drugs, cryptocurrencies have become global transactional tools, allowing sellers, and dealers at different ends of the world to trade in complete privacy and with minimal risk of being caught by the authorities (Dupuis et al., 2023). It is believed that cryptocurrencies are analogs of digital cash because they offer ultimate privacy. It is said that cryptocurrencies are digital currency which the user can create and destroy according to the demand and its value is determined only by the balance between the supply and the demand in the market. In other words, cryptocurrencies are a decentralized peer-to-peer value system, accessible to all users and which allows everyone to perform all types of transactions safely. In particular, Bitcoin has attracted attention because of its value growth overcoming some financial crises, making this virtual currency an appealing tool to be used by criminal organizations in the narcotics trafficking business. The illegal drugs market is a worldwide phenomenon that is handled mainly by criminal organizations that can cause social, political, and economic impacts and, additionally, can be associated with other types of crime, making the international community intensify its efforts to cope with it. However, these organizations use money laundering to change their income from drug trafficking into assets that seem legitimized (Kabra & Gori, 2023).

- ***Cluster 6: cryptocurrency and human trafficking***

Human trafficking is defined as recruiting, harboring, transporting, providing, or obtaining a person for compelled labor or commercial sex acts through the use of

force, fraud, or coercion, or any means for the indication of subjection to involuntary servitude, peonage, debt bondage, or slavery. Human trafficking is a global problem that affects millions of people. The victims have forced labor in their gross domestic product, while a significant percentage of victims in the commercial sex industry are women and girls subjected to sex trafficking, forced marriage, and the sale of human organs. Given the prevalence of cash transactions in human trafficking, cryptocurrencies are often chosen due to the challenges in tracking financial movements across international borders (Kethineni & Cao, 2020; Sarkar & Shukla, 2023; Szakonyi et al., 2021; Visvizi et al., 2023). Child sexual exploitation not only harms the victim but also exploits the vulnerabilities of one of the most vulnerable groups in our society (Benavente et al., 2022; Josenhans et al., 2020; Laird et al., 2023; Wood, 2020). Legislation addressing human trafficking has explicitly criminalized the facilitation of children's involvement in sex work, with the aim of enhancing monitoring and combating this egregious crime. This criminalization is a critical component in the evaluation of cryptocurrencies' role in facilitating organized crime (Gerry & Shaw, 2019; Szakonyi et al., 2021).

- ***Cluster 7: cryptocurrency and corruption***

Corruption is typified by rigged procedures, illegal practices of public officeholders, and coalitions against the public interest. The corruption risks involving cryptocurrencies are linked to the existence of a collateral market that involves the financial intermediaries used to convert cryptocurrencies to real currencies. Corrupt public officials may be tempted to invest part of their illegal income in cryptocurrencies to conceal the stolen funds derived from their corrupt activities. The exchange of cryptocurrencies for real money can be used to conceal money derived from illegal activities and is supposedly laundered (Howson & de Vries, 2022; Kethineni & Cao, 2020; Vaz & Brown, 2020).

While the criminal use of cryptocurrencies can have negative effects on security and market trust, the corruption fully related to cryptocurrency functions is currently limited. It is linked to the acceptance of new technologies, limitations of new public administrators, and a higher knowledge of cryptocurrencies, rather than cryptocurrency features, which make cryptocurrency functions especially corrupt. This does not mean that cryptocurrencies are corruption-resistant (Kaplan, 2021; Nabilou, 2020; Wronka, 2023).

4.2 Analysis of the results

Cryptocurrencies have increasingly become a subject of interest, especially driven by both technology and security management perspectives. With the rapid growth of FinTech, digital transactions and payments are gaining public trust, but are also providing opportunities for cybercrime to misuse the digital channel that merges cash and technology (Dupuis & Gleason, 2021; Teichmann, 2022). Financial technologies are accelerating the development of various official financial partnerships,

commercial exchanges, and voluntary networks that help to leverage legal entities with innovative processes that benefit economies. However, the development of FinTech has also led to new competitors in the shark pool, and their exploitative actions in the world of cybercriminals raise legal, moral, and ethical concerns. Both legitimate and criminal activities revolve around digital currencies that are maintained and managed online, providing security to trading parties under pseudonyms, while also allowing them to operate or conduct business transactions across borders without any legal oversight or ownership. These futuristic financial ideas can be a catalyst for criminal aspirations, which can corrupt vast numbers of citizens and disrupt a country's national security policies (Badawi & Jourdan, 2020; Wronka, 2024).

The risks associated with cryptocurrency use and its high-profile status may act as a deterrent to the systematic benefit derived by criminal organizations from digital coin mechanisms (Lin, 2024; Sanz-Bas et al., 2021).

The use of cryptocurrencies by organized crime remains a subject that has received limited attention in the extant literature and is frequently overlooked by international bodies. While the adoption of cryptocurrencies by criminal organizations remains in its early stages, they have emerged as a formidable instrument for diversifying the financial gains derived from a wide range of illicit activities. Notably, Bitcoin, despite its widespread popularity, continues to predominate as the primary medium for financial gain from the illicit activities most frequently associated with criminal organizations and terrorist entities (Bertola, 2020; Kabra & Gori, 2023; Kutera, 2022). Nevertheless, privacy coins have emerged as robust solutions for money laundering, facilitating the concealment of criminal proceeds and evasion of international sanctions. These digital currencies offer a high degree of anonymity, surpassing the security provided by traditional financial intermediaries. In the context of financial operations, cryptocurrency has emerged as a significant medium for criminal organizations (Bjelajac & Bajac, 2022; Tronnier, 2021; Wronka, 2023), often serving as a means to facilitate transactions that would otherwise be subject to scrutiny by financial regulatory authorities. The use of cryptocurrency and the absence of regulatory oversight can effectively minimize the need for a network of intermediaries involved in the control of illicit conduct. This is particularly evident when blockchain technology is employed, as it obscures the link between the customer and their account or transaction. Tax fraud is identified as a key reason for black market corruption and organized crime utilizing cryptocurrencies. The distinction between money laundering and tax evasion lies in the absence of a tangible foundation in the former, as opposed to the latter, which often stems from criminal or illicit activities that subsequently give rise to tax fraud (Kurauone et al., 2021; Otusanya & Adeyeye, 2022; Pițu et al., 2021; Samiilenko et al., 2021). It has been observed that officials are having trouble identifying transactions underpinning cryptocurrency due to privacy banks might hide behind. The use of tax havens by companies and local authorities is exposing secret properties as never before, making the proceeds of tax evasion visible. Money laundering hides the proceeds of illegal activities from the authorities, such as prostitution and drug supply, as well as tax evasion in order to escape prosecution. Using the blockchain as a tax evasion prevention device has been suggested, clarifying the linked transactions so as to be able to follow the cryptocurrencies. In this way, the taxpayer will incriminate themselves

and/or bring assets into the open that would otherwise be hidden from tax authorities (Goodell et al., 2021; Wronka, 2023). Exploring these various components is of both social and practical interest. The misuse of cryptocurrency is increasingly becoming a growing concern for policymakers and law enforcement agencies worldwide (Arnone, 2024; Trozze et al., 2022; Wronka, 2024).

4.3 Risks associated with cryptocurrency (mis)use

The misuse of cryptocurrency can pose several risks, including financial risks, cybersecurity risks, and systemic risks. The users who lose custody of their cryptocurrencies or are defrauded may suffer substantial losses, depending on the scale of their involvement and the price of the cryptocurrency at the time of the incident. Illicit actors can create fraudulent investment opportunities, directly steal funds from investors to finance a lavish lifestyle, or deceive victims into sending cryptocurrency under false pretenses (Badawi & Jourdan, 2020; Kutera, 2022).

In fact, the same cryptocurrency markets can also contribute to economic instability. The price and market capitalization of cryptocurrencies can exhibit extreme volatility, with prices sometimes fluctuating by tens of percentage points within a matter of hours or days. Typical directives such as expanding geopolitical tensions, unfavorable news stories about community debates, and adverse regulations or enforcement actions can contribute to rapid sell-offs and subsequent market instability (Ghorbel & Jeribi, 2021; Leirvik, 2022; Taskinsoy, 2020; Wang & Chong, 2021). These factors are compounded by a high risk of spam, since unsupervised or malicious regulators and actors can take advantage of market sentiment to induce widespread panic selling and further destabilize a particular digital currency. Due to the interconnectedness of the cryptocurrency markets and the broader global financial system, sustained market instability from large-scale fraud could risk spilling over into the broader economy. Any regulation that can help prevent cryptocurrency fraud is likely to affect financial stability and have trade-offs. A comprehensive understanding of the associated risks is therefore essential for all stakeholders, but especially for law enforcement and regulators who are working to develop responses to cryptocurrency risks. Without a comprehensive understanding, policy responses may only partially address the problem or create new ones (Almagsoosi et al., 2022; Ghosh et al., 2020; Özdemir, 2022). Ultimately, distinguishing the harm and the causes of this burgeoning market will help policymakers address important regulatory changes and could also potentially inform interventions targeted to this growing group of digital asset users. The financial risks posed by trading and use of cryptocurrencies are a central point of concern for regulatory authorities internationally (Aji & Adawiyah, 2022). More specifically, the potentially promising returns generated by the market have in part resulted in considerable losses for both individuals and organizations. While various fraudulent schemes frequently utilized in cryptocurrency markets are widely employed in other markets, financial capital is vulnerable to laundering and illicit financing via digital asset networks due to the cyber-based nature of the market. A report analyzing Ponzi schemes found that a significant percentage of these were associated with cryptocurrencies, with victims

losing billions of dollars (Gil-Cordero et al., 2024; Teng & Khong, 2021). The other fraudulent schemes frequently found in cryptocurrency markets, which also apply to other markets, include pump-and-dump and phishing activities. These schemes are adopted by fraudsters due to their ease of execution in the cyber sphere. Volatility represents a critical risk, interconnected with liquidity and investor protection. The low levels of liquidity that precipitate elevated costs of trading concomitantly engender heightened volatility and subsequent concentration, which can exert deleterious effects on an asset across multiple dimensions (Giudici et al., 2020; Luchkin et al., 2020; Smutny et al., 2021).

The increased use of digital wallets for cryptocurrency storage has made these platforms increasingly attractive targets for criminal actors. In account-based systems, the theft or loss of a private key often leads to the irreversible loss of cryptocurrency. Additionally, identity theft is a major concern, as many platforms rely on email addresses for login and password recovery, often without strong security measures in place. A significant challenge stems from the fact that many cryptocurrency investors have limited technical expertise and may not implement adequate security precautions. Moreover, most cryptocurrency communities and discussion boards lack comprehensive cybersecurity protocols, further exacerbating the risks (Castonguay & Stein Smith, 2020; Mikhaylov, 2023).

4.4 Regulatory concerns and law-enforcement challenges

Cryptocurrencies, as decentralized and global financial innovations, present significant challenges for international regulators due to varying national approaches. While some countries have embraced blockchain and digital currencies for legal transactions, others have imposed outright bans, prohibiting residents from engaging in crypto-related activities. A third group permits limited use but warns against investments in digital assets. This heterogeneity in regulatory approaches impedes the establishment of effective international cooperation, consequently hindering the alignment of legal frameworks to address the criminal misuse of digital assets (Sanz-Bas et al., 2021). The absence of a harmonized regulatory framework gives individual nations the opportunity to establish their own norms, which often results in the stifling of innovation due to the complexity and cost of administrative processes. Regulators face the dual challenge of fostering innovation to promote economic growth while preventing unauthorized use, including criminal activities, within country-specific regulatory frameworks.

Cryptocurrencies have attracted the interest of private enterprises, governments, and regulatory bodies worldwide. Regulatory approaches differ globally, with some nations welcoming blockchain-based industries, including initial coin offerings (ICOs) and cryptocurrency exchanges, while others resist adoption. Central banks, wary of losing control over monetary systems, prefer centralized financial services like banks and securities depositories for cost-effective and reliable operations (Ferreira et al., 2021). This reluctance has contributed to legal and regulatory challenges, particularly in curbing criminal activities such as money laundering, arms trafficking, and drug trade (Uzougbo et al., 2024; Olabanji, 2023). The regulatory

frameworks governing cryptocurrencies vary widely across national and international contexts, ranging from light-touch self-regulation to robust systems requiring licensing and enforcement by regulatory agencies. In deregulated or under-regulated jurisdictions, criminal abuses often occur, driven by insufficient oversight or carelessness by businesses. Conversely, stricter regimes actively combat abuses, with well-resourced teams addressing illicit behavior (Bellavitis et al., 2021; Ozili, 2022). Weak regulatory frameworks are susceptible to exploitation, highlighting the need to identify and strengthen loopholes. A well-calibrated regime not only curtails abuse but also builds confidence, encouraging societal and corporate adoption of blockchain technologies. Balancing innovation and safety is crucial for consumer protection and alleviating the resource burdens on regulatory agencies (Alfieri, 2022; Kayani & Hasan, 2024).

Cryptocurrencies, developed by private actors, often operate contrary to societal interests, posing economic and social risks. Strong regulation has the potential to address these risks without undermining cryptocurrency principles such as neutrality, individualism, and property rights. Advisory groups and public-private partnerships play a vital role in finding solutions to these challenges (Al-Tawil, 2023; Feinstein & Werbach, 2021).

A global overview of cryptocurrency regulation reveals that it is influenced by a combination of political, legal, and cultural factors. The policymakers face the challenging task of ensuring consumer protections while fostering innovation. Stakeholders must understand the varied regulatory frameworks to promote legal certainty (Ferreira & Sandner, 2021; Huang, 2021; Silva & Mira da Silva, 2022; Wronka, 2024). Key legal interpretations include whether crypto-assets qualify as financial instruments or fall under prospectus regulations, as well as liability for losses. Limited case law exists, as technological advancements outpace judicial systems. Although pseudonymity and anonymity are not illegal, they complicate criminal investigations, preventing transaction monitoring and ownership assessment. The decentralized nature of cryptocurrencies enables anonymity, making law enforcement efforts to track and prosecute crimes challenging (Teichmann, 2022; Uzougbo et al., 2024).

The inherent characteristics of cryptocurrencies, namely their virtual nature, absence of standardized legislation, and the use of pseudonymity, render them susceptible to misuse, particularly by criminal organizations. The absence of centralized oversight in cryptocurrency systems enables illicit activities, such as money laundering and the funding of illegal operations. These features make gathering evidence, tracking suspects, and prosecuting offenders difficult. Criminals often employ off-chain transactions and break larger sums into smaller ones, further complicating enforcement efforts (Chawki, 2022; Kreminskyi et al., 2021).

Collaboration among regulatory agencies and private institutions is essential to address suspicious cryptocurrency transactions effectively. Training and cooperation between law enforcement and compliance teams enhance detection and prevention efforts. However, broader issues remain, including the lack of a comprehensive legal framework for tackling crypto-related crimes. The proposed regulations could include trusted intermediaries holding user data to ensure accountability while respecting privacy. Such measures would enable law enforcement to link users to

transactions and identify beneficial owners (de Haro-Olmo et al., 2020; Wu et al., 2020).

The cryptocurrency sector requires stronger enforcement mechanisms to prevent misuse while supporting innovation. The educational efforts for regulators, law enforcement, and financial institutions are critical to enhancing awareness and understanding of the evolving crypto landscape. The compliance teams must establish best practices and collaborate with law enforcement to address vulnerabilities (Al-Tawil, 2023; Pocher et al., 2023). Despite progress, significant challenges remain in creating a criminal justice framework capable of addressing cryptocurrency-related crimes. The absence of agreed standards in the financial industry complicates enforcement, necessitating capacity-building measures across jurisdictions. The establishment of clear regulatory guidelines and international cooperation will be essential in tackling the misuse of cryptocurrencies (Sarkar & Shukla, 2023; Shonhadji & Maulidi, 2022).

In conclusion, cryptocurrencies pose a set of regulatory, legal, and enforcement challenges due to their decentralized and pseudonymous nature. To address these challenges, regulatory frameworks must strike a balance between fostering innovation and ensuring security and consumer protection. Strong collaboration among stakeholders (regulators, law enforcement, and private institutions) can mitigate risks and build a robust framework for the cryptocurrency sector (Covolo, 2020; Wronka, 2023).

4.5 Practical proposals and policy implications

This review reveals several actionable insights with practical implications for policymakers, law enforcement, and compliance officers. The following proposals, grounded in the literature reviewed, aim to bridge the gap between academic knowledge and real-world application:

- Integration of blockchain forensic tools: law enforcement and financial institutions should invest in blockchain analysis platforms such as Chainalysis, Elliptic, or CipherTrace. These tools enable transaction tracking, address clustering, and pattern recognition to trace illicit flows more effectively. Their implementation can substantially reduce investigation time and increase conviction rates in crypto-related cases.
- Creation of Crypto-Compliance Units: Regulatory agencies and national FIUs (Financial Intelligence Units) should establish specialized units focused on cryptocurrency-related financial crimes. These units should be trained in crypto-forensics and collaborate with exchanges to monitor suspicious transactions.
- Mandatory KYC/AML standards across jurisdictions: a global regulatory framework that mandates uniform Know-Your-Customer (KYC) and Anti-Money Laundering (AML) standards for all crypto exchanges and wallet providers is necessary. This could be modeled after FATF's Travel Rule and would help mitigate regulatory arbitrage across countries.

- Use of smart contracts for lawful traceability: governments and developers could explore the integration of legal "flags" in smart contracts to enable audit trails and regulatory oversight for high-risk transactions, while respecting privacy frameworks such as GDPR.
- Proactive regulation of privacy coins: coins with enhanced anonymity features (e.g., Monero, Zcash) should be subject to stricter regulatory scrutiny or transactional thresholds. Exchanges' listing such assets must report transaction volumes and comply with disclosure obligations.
- Public–private intelligence sharing platforms: encouraging data-sharing partnerships between crypto exchanges, law enforcement, and tech providers can significantly enhance detection capabilities and build an intelligence-led enforcement ecosystem.

These proposals reflect the thematic findings from the systematic review and are aligned with the stated hypothesis that the technological features of cryptocurrencies create persistent enforcement and regulatory challenges. Their adoption could reduce the operational space for criminal exploitation of digital assets.

5 Conclusions

The paper offers a systematic review on the (mis)use of cryptocurrencies by criminal organizations, with the objective of fostering shared awareness among all relevant stakeholders.

The analysis revealed that the technical features of cryptocurrencies—decentralization, pseudo-anonymity, and cross- border operability—make them uniquely suited to enable various forms of illicit activity, including money laundering, ransomware, cybercrime, and trafficking. The cryptocurrencies have the potential to be misused in various illicit activities due to their unique characteristics, including pseudo-anonymity, decentralization, and cross-border characteristics. However, disrupting and dismantling cryptocurrency misuse poses significant technical and legal challenges. The rapid evolution of cryptocurrency means that initial research and even standardization may become outdated within a few years. The examples of noteworthy incidents include ransomware, exchange fraud, theft, and money laundering. Law enforcement and regulatory agencies at the national and international levels face difficulties in developing law enforcement and regulatory responses at the same pace as the technology evolves. In order to develop and implement effective regulations and police responses, it is essential to understand the opportunities and challenges posed by crypto-economic systems. The growing adoption and use of cryptocurrencies for various forms of criminal exploitation have posed significant law enforcement challenges. Our research investigated the intersection of cryptocurrencies, criminal economies, laws, and law enforcement. To this end, we identified a series of challenges and risks that influence law enforcement and the broader cryptocurrency regulatory ecosystem. Future research should include large-scale empirical studies of cryptocurrency misuse across varying jurisdictions. These studies would help to provide a better understanding of how regulatory powers may be developed

to limit (mis)use. Despite improvements in transaction monitoring and tracking approaches and further innovative developments of techniques, more research is required (Covolo, 2020; Kutera, 2022).

The originality of this work lies in its structured, interdisciplinary synthesis of empirical findings across financial, technological, and legal domains. This approach fills a critical gap in the existing literature, where most studies either focus narrowly on legal regulation or adopt a purely technical perspective. Our results confirm the hypothesis that the unique architecture of cryptocurrencies creates persistent challenges for enforcement and regulation, which are further exacerbated by jurisdictional fragmentation (Badawi & Jourdan, 2020; Dupuis & Gleason, 2021; Guidara, 2022; Leuprecht et al., 2023; Wronka, 2022).

In addition, to offering theoretical insights, the study outlines a series of concrete, actionable proposals, presented in a dedicated results subsection. These include the integration of blockchain forensic tools, mandatory KYC/AML harmonization, and the creation of specialized regulatory units. Together, these measures reflect a shift from reactive to proactive governance, aiming to balance innovation with robust security measures. In particular, this study offers relevant information on the implications of cryptocurrencies in relation to criminal organizations and is useful from both theoretical and practical perspectives. In the scientific domain, this paper contributes to the understanding of the (mis)use of cryptocurrencies in illicit transactions by criminal organizations, emphasizing the discrepancies involved in the treatment of illicit transactions with the use of cryptocurrencies, stressing that traditional measures are insufficient to also fight the technological problems where, nowadays, criminals operate (Adiyatma & Maharani, 2020; Gonzálvez-Gallego & Pérez-Cárceles, 2021; Leuprecht et al., 2023). Although not all cryptocurrency users engage in criminal activities, and not all criminal activities involve cryptocurrency, the lack of regulation, anonymity, and decentralization have created ample opportunities for criminals (Dhali et al., 2023; Galit et al., 2024; Kethineni & Cao, 2020; Kirimhan, 2023; Uzougbo et al., 2024; Watters, 2023).

The findings hold substantial relevance for policymakers, law enforcement, regulators, and scholars. They demonstrate that addressing the misuse of cryptocurrencies requires not only updated technical tools but also a coordinated, cross-jurisdictional legal response and a rethinking of existing institutional capacities. As such, the paper contributes both to the academic discourse and to the formulation of evidence-based strategies to mitigate criminal abuse of digital assets. Greater availability of data and emerging partnerships will provide further and possibly improved evidence of cryptocurrency (mis)use and transformations in the methods and practices observed to have emerged (Akartuna et al., 2022; Allen et al., 2020; Dupuis et al., 2021; Galit et al., 2024; Kayani & Hasan, 2024).

This study reveals, however, that many policymaking agencies are still adopting a reactive response, concentrating on combating money laundering and terrorism financing. Crucially, regulatory innovation must also address the prevention of crime and proactive deterrence, while minimally disrupting the drive for technological innovation. The fast-changing cryptocurrency technological context, along with the growth of the phenomenon, makes the issue a multi-faceted one. Solutions to many of the vulnerabilities related to the use of cryptocurrencies require

actions from all involved stakeholders, including governments, exceeding the sphere of influence of traditional security measures. However, some specific solutions can be discussed in distinct technological domains. Their real-world feasibility, though, must be carefully considered, in some cases considering specific trade-offs between security and operational needs. As exchanges proliferate, trafficking becomes more efficient, driving down risk-adjusted trade. Furthermore, regulators should be particularly concerned about exchanges registered in jurisdictions with weak governance arrangements.

Nevertheless, while cryptocurrencies offer significant benefits such as reduced transaction costs and financial inclusion, they also pose ethical challenges like facilitating illegal activities and financial instability, necessitating a comprehensive ethical framework and careful regulation to balance these aspects (Dierksmeier & Seele, 2018). Further integration of legal, criminological, and technological perspectives will be key to navigating the evolving crypto-criminal landscape.

6 Limitations and recommendations for future research

Despite the growing interest in how criminal organizations exploit cryptocurrencies for illicit activities, significant research and regulatory gaps persist. Furthermore, several limitations remain, necessitating further exploration (Dupuis & Gleason, 2021; Wronka, 2023).

The relationship between autonomous trafficking and its dependence on low-skill, high-security cybercrimes like ransomware warrants deeper analysis. Future research should explore the development of technology specifically designed for criminal activities and its broader implications for global security. Furthermore, as cryptocurrencies evolve, they may be supplanted by blockchain-based digital artifacts, shifting the focus of illicit transactions. This transition calls for studies that explore the emerging "blockchain arms race" and its economic and legal ramification (Limba et al., 2020; Sanz-Bas et al., 2021; Shortis et al., 2020). Moreover, the role of economic incentives in combating cryptocurrency-enabled crime also warrants closer examination. Specifically, research should focus on the regulatory chokepoints presented by cryptocurrency exchanges, emphasizing the necessity for international cooperation to standardize and enforce control measures. The effectiveness of situational crime prevention tailored to cryptocurrency misuse, alongside investigations into nation-state involvement in such activities, represents another promising area for future inquiry (Covolo, 2020; Gonzálvez-Gallego & Pérez-Cárceles, 2021).

A key limitation of the adopted systematic literature review (SLR) method lies in its dependence on already published academic sources. As such, the analysis is inherently limited to the scope, quality, and disciplinary biases of existing studies. This excludes valuable insights that may be found in gray literature, government reports, or classified investigative data not available in peer-reviewed journals. Furthermore, the choice to rely primarily on English-language publications may have introduced a linguistic and geographic bias, potentially omitting relevant research in other jurisdictions, especially non-Western countries

with rising crypto-crime rates. Another limitation is the exclusion of single-case studies and conference abstracts that may have presented detailed but narrowly scoped insights into emerging criminal patterns. While the PRISMA methodology ensures methodological rigor and replicability, it may sacrifice the depth and context provided by ethnographic, investigative, or real-time law enforcement data sources. Additionally, the qualitative nature of thematic clustering, while appropriate for synthesizing patterns, does not allow for quantitative validation or generalization of findings. These methodological boundaries, while necessary for transparency and consistency, imply that some aspects of cryptocurrency-enabled crime—particularly those involving rapidly changing technologies or underreported criminal networks—may remain underexplored in this review.

Technological advancements present valuable opportunities to tackle these challenges, with blockchain forensic tools and artificial intelligence showing significant potential in detecting and analyzing illicit activities. However, their effectiveness in real-time applications and widespread adoption by law enforcement and regulated sectors require further assessment. Future research should focus on developing best practices for businesses handling cryptocurrency and blockchain operations to enhance compliance and minimize misuse (Agarwal et al., 2024b; Akinbi et al., 2022; Hossain, 2023; Zarpala & Casino, 2021). Additionally, a critical area for investigation involves the balance between reducing anonymity in cryptocurrency transactions and maintaining operational utility: regulatory measures should target forms of cryptocurrencies most susceptible to misuse while recognizing the technology's potential to combat corruption and enhance transparency in vulnerable economies (Bahamazava & Nanda, 2022; Hossain, 2023; Kumari et al., 2021; Liu et al., 2021).

In conclusion, the scarcity of concrete case studies and judicial outcomes related to specific criminal organizations, such as the Italian Mafia, underscores the need for empirical research into their involvement in cryptocurrency-facilitated crimes. That might draw more attention to upcoming research that should focus on operational methodologies employed by investigators, procedural strategies, and the role of international entities like Europol and Eurojust in combating crypto- enabled criminal networks. By addressing these gaps, research can contribute to a nuanced understanding of the complex interplay between technological innovation, regulatory frameworks, and criminal exploitation (Cavallaro et al., 2020; Dagnes et al., 2020; Le Moglie & Sorrenti, 2022; Mirenda et al., 2022; Piemontese, 2023).

Acknowledgements The author would like to express sincere gratitude to Professor Costantino Visconti for his invaluable coordination of the project and continuous support throughout its development. Special thanks also go to Elena Virciglio for her preliminary assistance in revising the bibliography. This paper has been supported by the Italian Ministerial grant PRIN 2022 PNRR "Follow the money: criptocurrencies and criminal organizations" cod. U-GOV PRJ-1546—CUP: B53D23026310001.

Author contributions Dr. Gioia Arnone was responsible for collecting the materials and drafting the main manuscript. Dr. Giovanni Scire' contributed by designing and drafting the tables and charts, ensuring the clear presentation of data and key findings. Prof. Enzo Bivona provided a thorough revision of the entire paper, offering critical insights and refinements to enhance the clarity, coherence, and academic rigor of the study. All authors reviewed and approved the final version of the manuscript.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no competing interests.

References

Adiyatma, S. E., & Maharani, D. F. (2020). Cryptocurrency's Control in the Misuse of Money Laundering Acts as an Effort to Maintain the Resilience and Security of the State. *Lex Scientia Law Review, 4*(1), 75–88. https://doi.org/10.15294/lesrev.v4i1.38257

Agarwal, U., Rishiwal, V., Tanwar, S., & Yadav, M. (2024). Blockchain and crypto forensics: Investigating crypto frauds. *International Journal of Network Management*. https://doi.org/10.1002/nem.2255

Ahmed, A. A., & Alabi, O. O. (2024). Secure and scalable blockchain-based federated learning for cryptocurrency fraud detection: A systematic review. *IEEE Access, 12*, 102219–102241. https://doi.org/10.1109/ACCESS.2024.3429205

Aji, H. M., & Adawiyah, W. R. (2022). How e-wallets encourage excessive spending behavior among young adult consumers? *Journal of Asia Business Studies*. https://doi.org/10.1108/JABS-01-2021-0025

Akartuna, E. A., Johnson, S. D., & Thornton, A. (2022). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. *Technological Forecasting and Social Change*. https://doi.org/10.1016/j.techfore.2022.121632

Akcinaroglu, S., & Shi, M. (2023). Exploring the Impact of Cryptocurrency on Terrorism. *Terrorism and Political Violence*. https://doi.org/10.1080/09546553.2023.2275057

Akcinaroglu, S., & Shi, M. (2025). Exploring the Impact of Cryptocurrency on Terrorism. *Terrorism and Political Violence, 37*(1), 111–135. https://doi.org/10.1080/09546553.2023.2275057

Akinbi, A., MacDermott, Á., & Ismael, A. M. (2022). A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models. *Forensic Science International: Digital Investigation*. https://doi.org/10.1016/j.fsidi.2022.301470

Alfieri, C. (2022). Cryptocurrency and national security. *International Journal on Criminology*. https://doi.org/10.18278/ijc.9.1.3

Allen, D. W. E., Berg, C., Markey-Towler, B., Novak, M., & Potts, J. (2020). Blockchain and the evolution of institutional technologies: Implications for innovation policy. *Research Policy*. https://doi.org/10.1016/j.respol.2019.103865

Allen, F., Gu, X., & Jagtiani, J. (2022). Fintech, cryptocurrencies, and CBDC: Financial structural transformation in China. *Journal of International Money and Finance*. https://doi.org/10.1016/j.jimonfin.2022.102625

Almagsoosi, L. Q. K., Abadi, M. T. E., Hasan, H. F., & Sharaf, H. K. (2022). Effect of the volatility of the crypto currency and its effect on the market returns. *Industrial Engineering and Management Systems*. https://doi.org/10.7232/iems.2022.21.2.238

Alqudah, M., Ferruz, L., Martín, E., Qudah, H., & Hamdan, F. (2023). The sustainability of investing in cryptocurrencies: A bibliometric analysis of research trends. *International Journal of Financial Studies*. https://doi.org/10.3390/ijfs11030093

Al-Tawil, T. N. (2023). Anti-money laundering regulation of cryptocurrency: UAE and global approaches. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-07-2022-0109

Andrei, F., & Veltri, G. A. (2025). Signalling strategies and opportunistic behaviour: Insights from darknet markets. *PLoS ONE, 20*(3), Article e0319794. https://doi.org/10.1371/journal.pone.0319794

Andrianova, A. (2020). Countering the financing of terrorism in the conditions of digital economy. *Advances in Intelligent Systems and Computing*, *908*. https://doi.org/10.1007/978-3-030-11367-4_2

Arnone, G. (2024). *Navigating the world of cryptocurrencies: Technology, economics, regulations, and future trends*. Springer Nature.

Badawi, E., & Jourdan, G. V. (2020). Cryptocurrencies emerging threats and defensive mechanisms: A systematic literature review. *IEEE Access, 8*, 200021–200037. https://doi.org/10.1109/ACCESS.2020.3034816

Bahamazava, K., & Nanda, R. (2022). The shift of DarkNet illegal drug trade preferences in cryptocurrency: The question of traceability and deterrence. *Forensic Science International: Digital Investigation*. https://doi.org/10.1016/j.fsidi.2022.301377

Barhate, B., & Dirani, K. M. (2022). Career aspirations of generation Z: a systematic literature review. *European Journal of Training and Development*. https://doi.org/10.1108/EJTD-07-2020-0124

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency scams: Analysis and perspectives. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3123894

Belke, A., & Beretta, E. (2020). From cash to central bank digital currencies and cryptocurrencies: a balancing act between modernity and monetary stability. *Journal of Economic Studies*. https://doi.org/10.1108/JES-07-2019-0311

Bellavitis, C., Fisch, C., & Wiklund, J. (2021). A comprehensive review of the global development of initial coin offerings (ICOs) and their regulation. *Journal of Business Venturing Insights*. https://doi.org/10.1016/j.jbvi.2020.e00213

Benavente, B., Díaz-Faes, D. A., Ballester, L., & Pereda, N. (2022). Commercial sexual exploitation of children and adolescents in Europe: A systematic review. *Trauma, Violence, and Abuse*. https://doi.org/10.1177/1524838021999378

Bertola, F. (2020). Drug trafficking on darkmarkets: How cryptomarkets are changing drug global trade and the role of organized crime. *American Journal of Qualitative Research*. https://doi.org/10.29333/ajqr/8243

Besenyő, J., & Gulyas, A. (2021). The effect of the dark web on the security. *Journal of Security and Sustainability Issues, 11*(1), 103–121. https://doi.org/10.47459/jssi.2021.11.7

Bhardwaj, A. (2024). *Insecure digital frontiers*. CRC Press. https://doi.org/10.1201/9781003515395

Bjelajac, Ž, & Bajac, M. (2022). Blockchain technology and money laundering. *Pravo - Teorija i Praksa*. https://doi.org/10.5937/ptp2202021b

Boell, S. K., & Cecez-Kecmanovic, D. (2015). On being 'Systematic' in Literature Reviews in IS. *Journal of Information Technology, 30*(2), 161–173. https://doi.org/10.1057/jit.2014.26

Bonkile, M. P., Awasthi, A., Lakshmi, C., Mukundan, V., & Aswin, V. S. (2018). A systematic literature review of Burgers' equation with recent advances. *Pramana, 90*(6), 69. https://doi.org/10.1007/s12043-018-1559-4

Braga, A. A., Brunson, R. K., Cook, P. J., Turchan, B., & Wade, B. (2021). Underground gun markets and the flow of illegal guns into the Bronx and Brooklyn: A mixed methods analysis. *Journal of Urban Health*. https://doi.org/10.1007/s11524-020-00477-z

Bright, D., Halsey, M., Goldsmith, A., & Goudie, S. (2023). "I Know a Guy and He's Got Guns Galore": Accessing crime guns in the australian illicit firearms market. *Deviant Behavior*. https://doi.org/10.1080/01639625.2022.2086838

Bublyk, Y., Borzenko, O., & Hlazova, A. (2023). Cryptocurrency energy consumption: Analysis, global trends and interaction. *Environmental Economics*. https://doi.org/10.21511/ee.14(2).2023.04

Buil-Gil, D., & Saldaña-Taboada, P. (2022). Offending concentration on the internet: an exploratory analysis of bitcoin-related cybercrime. *Deviant Behavior*. https://doi.org/10.1080/01639625.2021.1988760

Cartwright, S., Liu, H., & Raddats, C. (2021). Strategic use of social media within business-to-business (B2B) marketing: A systematic literature review. *Industrial Marketing Management*. https://doi.org/10.1016/j.indmarman.2021.06.005

Castonguay, J., & Stein Smith, S. (2020). Digital assets and blockchain: hackable, fraudulent, or just misunderstood?*. *Accounting Perspectives*. https://doi.org/10.1111/1911-3838.12242

Cavallaro, L., Ficara, A., De Meo, P., Fiumara, G., Catanese, S., Bagdasar, O., Song, W., & Liotta, A. (2020). Disrupting resilient criminal networks through data analysis: The case of Sicilian Mafia. *PLoS ONE, 15*(8), Article e0236476. https://doi.org/10.1371/journal.pone.0236476

Chawki, M. (2022). Cybercrime and the Regulation of Cryptocurrencies. *Lecture Notes in Networks and Systems*, *439 LNNS*. https://doi.org/10.1007/978-3-030-98015-3_48

Chawla, S., & Mehta, K. (2023). *Cryptocurrency adoption in the era of industry 5.0* (pp. 240–262). https://doi.org/10.4018/978-1-6684-6403-8.ch013

Chen, X. H., Sarker, P. K., & Lau, C. K. M. (2025). *The impact of trust in cryptocurrency connectedness and realized volatility: Exploring the role of cybersecurity and investor sentiment*. https://doi.org/10.2139/ssrn.5128802

Cherniei, V., Cherniavskyi, S., Babanina, V., & Tykho, O. (2021). Criminal liability for cryptocurrency transactions: Global experience. *European Journal of Sustainable Development*. https://doi.org/10.14207/ejsd.2021.v10n4p304

Chiarini, A. (2020). Industry 4.0, quality management and TQM world. A systematic literature review and a proposed agenda for further research. *TQM Journal*. https://doi.org/10.1108/TQM-04-2020-0082

Chitsungo, C. (2024). Harnessing digital strategies to combat cryptocurrency-enabled crimes: addressing money laundering, illicit trade, and cyber threats. *American Journal of International Relations, 9*(7), 77–106. https://doi.org/10.47672/ajir.2523

Chlebowicz, P., & Buczyński, S. (2023). Tracing the shadows: Inside the European illegal arms market—the case of Poland. *Archiwum Kryminologii, 45*(1), 75–113. https://doi.org/10.7420/AK2023.03

Choi, D., Chung, C. Y., Seyha, T., & Young, J. (2020). Factors affecting organizations' resistance to the adoption of blockchain technology in supply networks. *Sustainability (Switzerland)*. https://doi.org/10.3390/su12218882

Cohen, D., Te'eni, D., Yahav, I., Zagalsky, A., Schwartz, D., Silverman, G., Mann, Y., Elalouf, A., & Makowski, J. (2025). Human–AI enhancement of cyber threat intelligence. *International Journal of Information Security, 24*(2), 99. https://doi.org/10.1007/s10207-025-01004-4

Collins, C., Dennehy, D., Conboy, K., & Mikalef, P. (2021). Artificial intelligence in information systems research: A systematic literature review and research agenda. *International Journal of Information Management*. https://doi.org/10.1016/j.ijinfomgt.2021.102383

Cong, W., Harvey, C., Rabetti, D., & Wu, Z.-Y. (2025). An anatomy of crypto-enabled cybercrimes. *Management Science*. https://doi.org/10.1287/mnsc.2023.03691

Courtois, N. T., Gradon, K. T., & Schmeh, K. (2021). *Crypto currency regulation and law enforcement perspectives*. http://arxiv.org/abs/2109.01047

Covolo, V. (2020). The EU response to criminal misuse of cryptocurrencies: The young, already outdated 5th anti- money laundering directive. *European Journal of Crime, Criminal Law and Criminal Justice,*. https://doi.org/10.1163/15718174-bja10003

Crossan, M. M., & Apaydin, M. (2010). A multi-dimensional framework of organizational innovation: A systematic review of the literature. *Journal of Management Studies, 47*(6), 1154–1191. https://doi.org/10.1111/j.1467-6486.2009.00880.x

Cunha, P. R., Melo, P., & Sebastião, H. (2021). From bitcoin to central bank digital currencies: Making sense of the digital money revolution. *Future Internet*. https://doi.org/10.3390/fi13070165

Custers, B., Oerlemans, J.-J., & Pool, R. (2020). Laundering the Profits of Ransomware. *European Journal of Crime, Criminal Law and Criminal Justice,*. https://doi.org/10.1163/15718174-02802002

Cusumano, M. A. (2024). Private crypto versus public digital. *Communications of the ACM, 67*(10), 22–25. https://doi.org/10.1145/3685761

Dagnes, J., Donatiello, D., Moiso, V., Pellegrino, D., Sciarrone, R., & Storti, L. (2020). Mafia infiltration, public administration and local institutions: A comparative study in Northern Italy. *European Journal of Criminology, 17*(5), 540–562. https://doi.org/10.1177/1477370818803050

Dayoub, B., Yang, P., Omran, S., Zhang, Q., & Dayoub, A. (2024). Digital silk roads: Leveraging the metaverse for cultural tourism within the belt and road initiative framework. *Electronics, 13*(12), 2306. https://doi.org/10.3390/electronics13122306

de Haro-Olmo, F. J., Varela-Vaca, Á. J., & Álvarez-Bermejo, J. A. (2020). Blockchain from the perspective of privacy and anonymisation: A systematic literature review. *Sensors (Switzerland)*. https://doi.org/10.3390/s20247171

Dhali, M., Hassan, S., Mehar, S. M., Shahzad, K., & Zaman, F. (2023). Cryptocurrency in the Darknet: sustainability of the current national legislation. *International Journal of Law and Management*. https://doi.org/10.1108/IJLMA-09-2022-0206

Dierksmeier, C., & Seele, P. (2018). Cryptocurrencies and Business Ethics. *Journal of Business Ethics*. https://doi.org/10.1007/s10551-016-3298-0

Dulisse, B. C., Connealy, N., & Logan, M. W. (2024). "Get rich quick", scheme or script? The effect of cryptoculture on the susceptibility of fraud victimization among cryptocurrency purchasers. *Journal of Criminal Justice*. https://doi.org/10.1016/j.jcrimjus.2024.102273

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

Dupuis, D., Gleason, K. C., & Kannan, Y. H. (2021). Bitcoin and beyond: crypto asset considerations for auditors. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3903995

Dupuis, D., Smith, D., & Gleason, K. (2023). Old frauds with a new sauce: Digital assets and space transition. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-11-2021-0242

Faccia, A., Moçteanu, N. R., Cavaliere, L. P. L., & Mataruna-Dos-Santos, L. J. (2020). Electronic money laundering, the dark side of Fintech: An overview of the most recent cases. In: *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3430279.3430284

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

Ferdous, M. S., Chowdhury, M. J. M., & Hoque, M. A. (2021). A survey of consensus algorithms in public blockchain systems for crypto-currencies. *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2021.103035

Ferreira, A., & Sandner, P. (2021). Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure. *Computer Law and Security Review*. https://doi.org/10.1016/j.clsr.2021.105632

Ferreira, A., Sandner, P., & Dünser, T. (2021). Cryptocurrencies, DLT and crypto assets—The road to regulatory recognition in Europe. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3891401

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies, 32*(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015

Fülöp, M. T., Ionescu, C. A., & Topor, D. I. (2024). Digital business world and ethical dilemmas: a systematic literature review. *Digital Finance*. https://doi.org/10.1007/s42521-024-00119-y

Fylaktou, G., & Savvides, C. (2025). Fraud, crime prevention and financial crime investigation in blockchain. In *Handbook of Blockchain Technology* (pp. 311–328). Edward Elgar Publishing. https://doi.org/10.4337/9781803922805.00032

Gainsbury, S. M., & Blaszczynski, A. (2017). How blockchain and cryptocurrency technology could revolutionize online gambling. *Gaming Law Review, 21*(7), 482–492. https://doi.org/10.1089/glr2.2017.2174

Galit, K., Djamchid, A., & Moti, Z. (2024). Fighting fire with fire: combating criminal abuse of cryptocurrency with a P2P Mindset. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-024-10498-7

Gerry Q.C., F., & Shaw, P. (2019). Emerging and future technology trends in the links between cybercrime, trafficking in persons and smuggling of migrants. In: *2019 First International Conference on Transdisciplinary AI (TransAI)*, 1–9. https://doi.org/10.1109/TransAI46475.2019.00009

Ghazi-Tehrani, A. K., & Pontell, H. N. (2021). Phishing evolves: Analyzing the enduring cybercrime. *Victims and Offenders*. https://doi.org/10.1080/15564886.2020.1829224

Ghorbel, A., & Jeribi, A. (2021). Investigating the relationship between volatilities of cryptocurrencies and other financial assets. *Decisions in Economics and Finance*. https://doi.org/10.1007/s10203-020-00312-9

Ghosh, A., Gupta, S., Dua, A., & Kumar, N. (2020). Security of Cryptocurrencies in blockchain technology: State-of- art, challenges and future prospects. *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2020.102635

Gil-Cordero, E., Ledesma-Chaves, P., Arteaga Sánchez, R., & Mariano, A. M. (2024). Crypto-wallets revolution! Key factors driving behavioral intention to adopt the Coinbase Wallet using mixed PLS-SEM/fsQCA methodology in the Spanish environment. *International Journal of Bank Marketing*. https://doi.org/10.1108/IJBM-01-2023-0035

Giudici, G., Milne, A., & Vinogradov, D. (2020). Cryptocurrencies: market analysis and perspectives. *Journal of Industrial and Business Economics*. https://doi.org/10.1007/s40812-019-00138-6

Gonzálvez-Gallego, N., & Pérez-Cárceles, M. C. (2021). Cryptocurrencies and illicit practices: The role of governance. *Economic Analysis and Policy*. https://doi.org/10.1016/j.eap.2021.08.003

Goodell, G., Al-Nakib, H. D., & Tasca, P. (2021). A digital currency architecture for privacy and owner-custodianship. *Future Internet*. https://doi.org/10.3390/fi13050130

Greco, F., & Greco, G. (2020). Organised crime: Underground economy and regulations to combat cybercrime. *European Journal of Political Science Studies*. https://doi.org/10.46827/ejpss.v4i1.935

Guarino, A., Grilli, L., Santoro, D., Messina, F., & Zaccagnino, R. (2022). To learn or not to learn? Evaluating autonomous, adaptive, automated traders in cryptocurrencies financial bubbles. *Neural Computing and Applications*. https://doi.org/10.1007/s00521-022-07543-4

Guidara, A. (2022). Cryptocurrency and money laundering: A literature review. *Corporate Law and Governance Review*. https://doi.org/10.22495/clgrv4i2p4

Hairudin, A., Sifat, I. M., Mohamad, A., & Yusof, Y. (2022). Cryptocurrencies: A survey on acceptance, governance and market dynamics. *International Journal of Finance and Economics*. https://doi.org/10.1002/ijfe.2392

Hamilton, R., & Leuprecht, C. (2024). *the crime-crypto nexus: Nuancing risk across crypto-crime transactions* (pp. 15–42). https://doi.org/10.1007/978-3-031-59543-1_2

Hemdani, M. G. K. (2025). *Cryptocurrencies and the dark web: A gateway to money laundering* (pp. 217–247). https://doi.org/10.1007/978-3-031-80557-8_10

Hendricks, S., & Mwapwele, S. D. (2024). A systematic literature review on the factors influencing e-commerce adoption in developing countries. *Data and Information Management*. https://doi.org/10.1016/j.dim.2023.100045

Holden, J. T. (2018). Trifling and Gambling With Virtual Money. *UCLA Entertainment Law Review*. https://doi.org/10.5070/LR8251039717

Hossain, M. S. (2021). What do we know about cryptocurrency? Past, present, future. *China Finance Review International*. https://doi.org/10.1108/CFRI-03-2020-0026

Hossain, M. Z. (2023). Emerging trends in forensic accounting: data analytics, cyber forensic accounting, cryptocurrencies, and blockchain technology for fraud investigation and prevention. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4450488

Hou, J., Wang, C., & Luo, S. (2020). How to improve the competiveness of distributed energy resources in China with blockchain technology. *Technological Forecasting and Social Change*. https://doi.org/10.1016/j.techfore.2019.119744

Howson, P., & de Vries, A. (2022). Preying on the poor? Opportunities and challenges for tackling the social and environmental threats of cryptocurrencies for vulnerable and low-income communities. *Energy Research and Social Science*. https://doi.org/10.1016/j.erss.2021.102394

Huang, S. S. (2021). Crypto assets regulation in the UK: an assessment of the regulatory effectiveness and consistency. *Journal of Financial Regulation and Compliance*. https://doi.org/10.1108/JFRC-06-2020-0062

Hulland, J., Baumgartner, H., & Smith, K. M. (2018). Marketing survey research best practices: Evidence and recommendations from a review of JAMS articles. *Journal of the Academy of Marketing Science, 46*(1), 92–108. https://doi.org/10.1007/s11747-017-0532-y

Ibrahim, N. M., Abu Bakar, M., Abdul Rahman, S. S., & Amrullah DRS Nasrul, M. (2024). Cryptocurrency as digital asset according to the Principles of Usul Al-fiqh: a Critical Analysis by Mohd Daud Bakar. In: *2024 3rd International Conference on Creative Communication and Innovative Technology (ICCIT)*, 1–6. https://doi.org/10.1109/ICCIT62134.2024.10701114

Ikegwu, C. (2023). Governance challenges faced by the Bitcoin ecosystem: The way forward. *International Journal of Cryptocurrency Research*. https://doi.org/10.51483/ijccr.3.2.2023.74-83

Jain, A. K., & Gupta, B. B. (2022). A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*. https://doi.org/10.1080/17517575.2021.1896786

Josenhans, V., Kavenagh, M., Smith, S., & Wekerle, C. (2020). Gender, rights and responsibilities: The need for a global analysis of the sexual exploitation of boys. *Child Abuse and Neglect*. https://doi.org/10.1016/j.chiabu.2019.104291

Kabra, S., & Gori, S. (2023). Drug trafficking on cryptomarkets and the role of organized crime groups. *Journal of Economic Criminology*. https://doi.org/10.1016/j.jeconc.2023.100026

Kaplan, A. (2021). Cryptocurrency and corruption: auditing with blockchain. In *Contributions to Finance and Accounting: Vol. Part F213*. https://doi.org/10.1007/978-3-030-72628-7_15

Kayani, U., & Hasan, F. (2024). Unveiling Cryptocurrency Impact on Financial Markets and Traditional Banking Systems: Lessons for Sustainable Blockchain and Interdisciplinary Collaborations. *Journal of Risk and Financial Management*. https://doi.org/10.3390/jrfm17020058

Kethineni, S., & Cao, Y. (2020). The rise in popularity of cryptocurrency and associated criminal activity. *International Criminal Justice Review, 30*(3), 325–344. https://doi.org/10.1177/1057567719827051

Kirimhan, D. (2023). Importance of anti-money laundering regulations among prosumers for a cyber-secure decentralized finance. *Journal of Business Research*. https://doi.org/10.1016/j.jbusres.2022.113558

Kirli, D., Couraud, B., Robu, V., Salgado-Bravo, M., Norbu, S., Andoni, M., Antonopoulos, I., Negrete-Pincetic, M., Flynn, D., & Kiprakis, A. (2022). Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renewable and Sustainable Energy Reviews*. https://doi.org/10.1016/j.rser.2021.112013

Kohtamäki, M., Rabetino, R., & Möller, K. (2018). Alliance capabilities: A systematic review and future research directions. *Industrial Marketing Management, 68*, 188–201. https://doi.org/10.1016/j.indmarman.2017.10.014

Koropogui, S. T., St-Jean, É., & Pepin, M. (2025). Experiential learning approaches in university entrepreneurship education: a systematic review. In: *Annals of Entrepreneurship Education and Pedagogy - 2025* (pp. 29–47). Edward Elgar Publishing. https://doi.org/10.4337/9781035325795.00010

Kraus, S., Breier, M., Lim, W. M., Dabić, M., Kumar, S., Kanbach, D., Mukherjee, D., Corvello, V., Piñeiro-Chousa, J., Liguori, E., Palacios-Marqués, D., Schiavone, F., Ferraris, A., Fernandes, C., & Ferreira, J. J. (2022). Literature reviews as independent studies: Guidelines for academic practice. *Review of Managerial Science, 16*(8), 2577–2595. https://doi.org/10.1007/s11846-022-00588-8

Kreminskyi, O., Kuzmenko, O., Antoniuk, A., & Smahlo, O. (2021). International cooperation in the investigation of economic crimes related to cryptocurrency circulation. *Estudios De Economia Aplicada*. https://doi.org/10.25115/eea.v39i6.5247

Krishnan, A. (2020). Blockchain empowers social resistance and terrorism through decentralized autonomous organizations. *Journal of Strategic Security*. https://doi.org/10.5038/1944-0472.13.1.1743

Kumari, S., Tyagi, A. K., & Rekha, G. (2021). Applications of blockchain technologies in digital forensics and threat hunting. In: *Recent trends in blockchain for information systems security and privacy*. https://doi.org/10.1201/9781003139737-12

Kurauone, O., Kong, Y., Mago, S., Sun, H., Famba, T., & Muzamhindo, S. (2021). Tax evasion, political/public corruption and increased taxation: evidence from Zimbabwe. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-07-2020-0133

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

Laird, J. J., Klettke, B., Hall, K., & Hallford, D. (2023). Toward a global definition and understanding of child sexual exploitation: The development of a conceptual model. *Trauma, Violence, and Abuse.* https://doi.org/10.1177/15248380221090980

Le Moglie, M., & Sorrenti, G. (2022). Revealing "Mafia Inc."? Financial crisis, organized crime, and the birth of new enterprises. *The Review of Economics and Statistics, 104*(1), 142–156. https://doi.org/10.1162/rest_a_00942

Leirvik, T. (2022). Cryptocurrency returns and the volatility of liquidity. *Finance Research Letters*. https://doi.org/10.1016/j.frl.2021.102031

Leonidou, P., Salamanos, N., Farao, A., Aspri, M., & Sirivianos, M. (2023). A qualitative analysis of illicit arms trafficking on Darknet marketplaces. *ACM International Conference Proceeding Series, 1*(1145/3600160), 3605087.

Leuprecht, C., Jenkins, C., & Hamilton, R. (2023). Virtual money laundering: Policy implications of the proliferation in the illicit use of cryptocurrency. *Journal of Financial Crime, 30*(4), 1036–1054. https://doi.org/10.1108/JFC-07-2022-0161

Lim, W. M. (2025). Systematic literature reviews: Reflections, recommendations, and robustness check. *Journal of Consumer Behaviour*. https://doi.org/10.1002/cb.2479

Limba, T., Driaunys, K., Stankevicius, A., & Andrulevicius, A. (2020). Cryptocurrency and national security: Peculiarities of interaction. *Transformations in Business & Economics, 19*(2), 42–59.

Lin, L. S. F. (2024). Blockchain and black economy: Cryptocurrency-related crimes and countermeasures 1. *Journal of Islamic, Social, Economics and Development, 9*, 128–1755. https://doi.org/10.55573/JISED.096120

Liu, M., & Dong, B. (2025). *Analysis of cryptocurrencies mixing services and its regulatory mechanism* (pp. 95–110). https://doi.org/10.1007/978-981-96-1414-1_7

Liu, X. F., Jiang, X. J., Liu, S. H., & Tse, C. K. (2021). Knowledge discovery in cryptocurrency transactions: A survey. *IEEE Access*. https://doi.org/10.1109/ACCESS.2021.3062652

Longa, F. E. A. (2025). Cryptocurrency and money laundering. *American Journal of Industrial and Business Management, 15*(02), 362–371. https://doi.org/10.4236/ajibm.2025.152017

Luchkin, A. G., Lukasheva, O. L., Novikova, N. E., Melnikov, V. A., Zyatkova, A. V., & Yarotskaya, E. V. (2020). *Cryptocurrencies in the global financial system: Problems and ways to overcome them*. https://doi.org/10.2991/aebmr.k.200730.077

Luong, H. T. (2023). Foundations and trends in the darknet-related criminals in the last 10 years: A systematic literature review and bibliometric analysis. *Security Journal*. https://doi.org/10.1057/s41284-023-00383-4

Macfarlane, E. (2021). Strengthening sanctions: Solutions to curtail the evasion of international economic sanctions through the use of cryptocurrency. *Michigan Journal of International Law*. https://doi.org/10.36642/mjil.42.1.strengthening

Machado, M., Coita, I. F., Gomez Teijeiro, L., Wenzlaff, K., Gregoriades, A., Themistocleous, C., van Heeswijk, W., Bernard, F. S., Muñiz, J. A., Bolesta, K., Osterrieder, J., Liu, Y., Dubrovska, A., Stanca, L., Aydin, N. S., Rupeika-Apoga, R., Teng, H.-W., Nur Yilmaz, G., Péliová, J., Filipovska, O. (2024). Crowdfunding fraud detection: A systematic review highlights ai and blockchain using topic modeling. https://doi.org/10.2139/ssrn.4948895

Mademlis, I., Mancuso, M., Paternoster, C., Evangelatos, S., Finlay, E., Hughes, J., Radoglou-Grammatikis, P., Sarigiannidis, P., Stavropoulos, G., Votis, K., & Papadopoulos, G. Th. (2023). *The invisible arms race: digital trends in illicit goods trafficking and AI-enabled responses*. https://doi.org/10.36227/techrxiv.24288703.v1

Martino, P. (2021). Blockchain and banking: how technological innovations are shaping the banking industry. In *Blockchain and banking: How technological innovations are shaping the banking industry*. https://doi.org/10.1007/978-3-030-70970-9

Marzo, G. D., Pandolfelli, F., & Servedio, V. D. P. (2022). Modeling innovation in the cryptocurrency ecosystem. *Scientific Reports*. https://doi.org/10.1038/s41598-022-16924-7

Maurushat, A., & Halpin, D. (2022). Investigation of Cryptocurrency Enabled and Dependent Crimes. In *Law, governance and technology series* (Vol. 47). https://doi.org/10.1007/978-3-030-88036-1_10

Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers and Security*. https://doi.org/10.1016/j.cose.2020.101762

Meng, L., Wen, K.-H., Brewin, R., & Wu, Q. (2020). Knowledge atlas on the relationship between urban street space and residents' health—A bibliometric analysis based on VOSviewer and CiteSpace. *Sustainability, 12*(6), 2384. https://doi.org/10.3390/su12062384

Mikhaylov, A., Danish, M. S. S., & Senjyu, T. (2021). A new stage in the evolution of cryptocurrency markets: Analysis by Hurst method. In *Strategic outlook in business and finance innovation: Multidimensional policies for emerging economies*. https://doi.org/10.1108/978-1-80043-444-820211004

Mikhaylov, A. (2023). Understanding the risks associated with wallets, depository services, trading, lending, and borrowing in the crypto space. *Journal of Infrastructure, Policy and Development.* https://doi.org/10.24294/jipd.v7i3.2223

Mirenda, L., Mocetti, S., & Rizzica, L. (2022). The economic effects of mafia: Firm level evidence. *American Economic Review, 112*(8), 2748–2773. https://doi.org/10.1257/aer.20201015

Mohamed Shaffril, H. A., Samsuddin, S. F., & Abu Samah, A. (2021). The ABC of systematic literature review: The basic methodological guidance for beginners. *Quality & Quantity, 55*(4), 1319–1346. https://doi.org/10.1007/s11135-020-01059-6

Momtaz, P. P. (2021). The pricing and performance of cryptocurrency. *European Journal of Finance*. https://doi.org/10.1080/1351847X.2019.1647259

Mugarura, N., & Ssali, E. (2020). Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-11-2019-0092

Mumford, D., Sampson, M., & Shires, J. (2024). The promises and pitfalls of cryptocurrencies and blockchain for marginalized communities. *Information, Communication & Society.* https://doi.org/10.1080/1369118X.2024.2391817

Nabilou, H. (2020). The dark side of licensing cryptocurrency exchanges as payment institutions. *Law and Financial Markets Review*. https://doi.org/10.1080/17521440.2019.1626545

Nali, M. C., Li, Z., Purushothaman, V., Larsen, M. Z., Cuomo, R. E., Yang, J. S., & Mackey, T. K. (2025). Identification of cannabis product characteristics and pricing on dark web markets. *Journal of Psychoactive Drugs*. https://doi.org/10.1080/02791072.2024.2446446

Nicholls, J., Kuppa, A., & Le-Khac, N. A. (2021). Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *IEEE Access, 9*, 163965–163986. https://doi.org/10.1109/ACCESS.2021.3134076

Nicholls, J., Kuppa, A., & Le-Khac, N. (2024). The next phase of identifying illicit activity in Bitcoin. *International Journal of Network Management*. https://doi.org/10.1002/nem.2259

Nizovtsev, Y. Y., Parfylo, O. A., Barabash, O. O., Kyrenko, S. G., & Smetanina, N. V. (2022). Mechanisms of money laundering obtained from cybercrime: the legal aspect. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-02-2021-0015

Nyhus, E. K., Frank, D. A., Król, M. K., & Otterbring, T. (2024). Crypto cravings: Gender differences in crypto investment intentions and the mediating roles of financial overconfidence and personality. *Psychology and Marketing*. https://doi.org/10.1002/mar.21921

Olabanji, S. O. (2023). Technological tools in facilitating cryptocurrency tax compliance: An exploration of software and platforms supporting individual and business adherence to tax norms. *Current Journal of Applied Science and Technology*. https://doi.org/10.9734/cjast/2023/v42i364239

Otusanya, O. J., & Adeyeye, G. B. (2022). The dark side of tax havens in money laundering, capital flight and corruption in developing countries: some evidence from Nigeria. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-02-2021-0044

Özdemir, O. (2022). Cue the volatility spillover in the cryptocurrency markets during the COVID-19 pandemic: evidence from DCC-GARCH and wavelet analysis. *Financial Innovation*. https://doi.org/10.1186/s40854-021-00319-0

Ozili, P. K. (2022). Decentralized finance research and developments around the world. *Journal of Banking and Financial Technology*. https://doi.org/10.1007/s42786-022-00044-x

Palmié, M., Wincent, J., Parida, V., & Caglar, U. (2020). The evolution of the financial technology ecosystem: An introduction and agenda for future research on disruptive innovations in ecosystems. *Technological Forecasting and Social Change*. https://doi.org/10.1016/j.techfore.2019.119779

Panda, S. K., Sathya, A. R., & Das, S. (2023). Bitcoin: Beginning of the Cryptocurrency Era. In *Intelligent Systems Reference Library* (Vol. 237, pp. 25–58). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-22835-3_2

Patsakis, C., Politou, E., Alepis, E., & Hernandez-Castro, J. (2024). Cashing out crypto: state of practice in ransom payments. *International Journal of Information Security*. https://doi.org/10.1007/s10207-023-00766-z

Piemontese, L. (2023). Uncovering illegal and underground economies: The case of mafia extortion racketeering. *Journal of Public Economics, 227*, Article 104997. https://doi.org/10.1016/j.jpubeco.2023.104997

Pițu, I. C., Ciocanea, B. C., & Petrașcu, D. (2021). Tax evasion-corrosive factor for the national economy. *European Journal of Interdisciplinary Studies*. https://doi.org/10.24818/ejis.2021.05

Pocher, N., Zichichi, M., Merizzi, F., Shafiq, M. Z., & Ferretti, S. (2023). Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics. *Electronic Markets*. https://doi.org/10.1007/s12525-023-00654-3

Rad, F. F., Oghazi, P., Palmié, M., Chirumalla, K., Pashkevich, N., Patel, P. C., & Sattari, S. (2022). Industry 4.0 and supply chain performance: A systematic literature review of the benefits, challenges, and critical success factors of 11 core technologies. *Industrial Marketing Management, 105*, 268–293. https://doi.org/10.1016/j.indmarman.2022.06.009

Radanliev, P. (2024). The rise and fall of cryptocurrencies: defining the economic and social values of blockchain technologies, assessing the opportunities, and defining the financial and cybersecurity risks of the Metaverse. *Financial Innovation*. https://doi.org/10.1186/s40854-023-00537-8

Samiilenko, H., Ivanova, N., Shaposhnykova, I., Vasylchenko, L., Solomakha, I., & Povna, S. (2021). Corruption as a threat to economic security of the country. *IJCSNS International Journal of Computer Science and Network Security*. https://doi.org/10.22937/IJCSNS.2021.21.12.44

Sangal, S., Duggal, G., & Nigam, A. (2024). Blockchain's double-edged sword: thematic review of illegal activities using blockchain. *Journal of Information, Communication and Ethics in Society*. https://doi.org/10.1108/JICES-04-2023-0061

Sanz-Bas, D., del Rosal, C., Náñez Alonso, S. L., & Echarte Fernández, M. Á. (2021). Cryptocurrencies and fraudulent transactions: Risks, practices, and legislation for their prevention in Europe and Spain. *Laws*. https://doi.org/10.3390/laws10030057

Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology, 2*, Article 100034. https://doi.org/10.1016/j.jeconc.2023.100034

Sarmento, M., & Simões, C. (2018). The evolving role of trade fairs in business: A systematic literature review and a research agenda. *Industrial Marketing Management, 73*, 154–170. https://doi.org/10.1016/j.indmarman.2018.02.006

Sauer, P. C., & Seuring, S. (2023). How to conduct systematic literature reviews in management research: A guide in 6 steps and 14 decisions. *Review of Managerial Science, 17*(5), 1899–1933. https://doi.org/10.1007/s11846-023-00668-3

Scharfman, J. (2024). Additional Cases and Trends in Cryptocurrency Fraud. In *The Cryptocurrency and Digital Asset Fraud Casebook, Volume II* (pp. 327–361). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-60836-0_12

Shan, S., Duan, X., Zhang, Y., Zhang, T. T., & Li, H. (2021). Research on collaborative governance of smart government based on blockchain technology: an evolutionary approach. *Discrete Dynamics in Nature and Society*. https://doi.org/10.1155/2021/6634386

Sharif, M. M., & Ghodoosi, F. (2022). The ethics of blockchain in organizations. *Journal of Business Ethics*. https://doi.org/10.1007/s10551-022-05058-5

Shonhadji, N., & Maulidi, A. (2022). Is it suitable for your local governments? A contingency theory-based analysis on the use of internal control in thwarting white-collar crime. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-10-2019-0128

Shortis, P., Aldridge, J., & Barratt, M. J. (2020). Drug cryptomarket futures: Structure, function and evolution in response to law enforcement actions. *In Research Handbook on International Drug Policy*. https://doi.org/10.4337/9781788117067.00031

Silva, E. C., & Mira da Silva, M. (2022). Research contributions and challenges in DLT-based cryptocurrency regulation: A systematic mapping study. *Journal of Banking and Financial Technology, 6*(1), 63–82. https://doi.org/10.1007/s42786-021-00037-2

Siqueira, A. C. O., Honig, B., Mariano, S., & Moraes, J. (2020). A Commons strategy for promoting entrepreneurship and social capital: Implications for community currencies, cryptocurrencies, and value exchange. *Journal of Business Ethics*. https://doi.org/10.1007/s10551-020-04578-2

Smith, D. (2024). *Virtual assets* (pp. 191–219). https://doi.org/10.1007/978-3-031-59842-5_13

Smutny, Z., Sulc, Z., & Lansky, J. (2021). Motivations, barriers and risk-taking when investing in cryptocurrencies. *Mathematics*. https://doi.org/10.3390/math9141655

Sokolov, K. (2021). Ransomware activity and blockchain congestion. *Journal of Financial Economics*. https://doi.org/10.1016/j.jfineco.2021.04.015

Steinmetz, F. (2023). The interrelations of cryptocurrency and gambling: Results from a representative survey. *Computers in Human Behavior, 138*, Article 107437. https://doi.org/10.1016/j.chb.2022.107437

Steinmetz, F., von Meduna, M., Ante, L., & Fiedler, I. (2021). Ownership, uses and perceptions of cryptocurrency: Results from a population survey. *Technological Forecasting and Social Change*. https://doi.org/10.1016/j.techfore.2021.121073

Szakonyi, A., Chellasamy, H., Vassilakos, A., & Dawson, M. (2021). *Using technologies to uncover patterns in human trafficking* (pp. 497–502). https://doi.org/10.1007/978-3-030-70416-2_64

Taskinsoy, J. (2020). Bitcoin Could Be the First Cryptocurrency to Reach a Market Capitalization of One Trillion Dollars. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3693765

Teichmann, F. M. (2022). Current trends in terrorist financing. *Journal of Financial Regulation and Compliance*. https://doi.org/10.1108/JFRC-03-2021-0022

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

Teng, S., & Khong, K. W. (2021). Examining actual consumer usage of E-wallet: A case study of big data analytics. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2021.106778

Tronnier, F. (2021). Privacy in Payment in the Age of Central Bank Digital Currency. In: *IFIP advances in information and communication technology*, *619 IFIP*. https://doi.org/10.1007/978-3-030-72465-8_6

Trozze, A., Davies, T., & Kleinberg, B. (2023). Explaining prosecution outcomes for cryptocurrency-based financial crimes. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-10-2021-0119

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*. https://doi.org/10.1186/s40163-021-00163-8

Uzougbo, N. S., Ikegwu, C. G., & Adewusi, A. O. (2024). International enforcement of cryptocurrency laws: Jurisdictional challenges and collaborative solutions. *Magna Scientia Advanced Research and Reviews, 11*(1), 068–083. https://doi.org/10.30574/msarr.2024.11.1.0075

van Eck, N. J., & Waltman, L. (2017). Citation-based clustering of publications using CitNetExplorer and VOSviewer. *Scientometrics, 111*(2), 1053–1070. https://doi.org/10.1007/s11192-017-2300-7

Vaz, J., & Brown, K. (2020). Sustainable development and cryptocurrencies as private money. *Journal of Industrial and Business Economics*. https://doi.org/10.1007/s40812-019-00139-5

Visvizi, A., Mora, H., & Varela-Guzman, E. G. (2023). The case of rWallet: A blockchain-based tool to navigate some challenges related to irregular migration. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2022.107548

Wang, H. M., & Hsieh, M. L. (2024). Cryptocurrency is new vogue: a reflection on money laundering prevention. *Security Journal*. https://doi.org/10.1057/s41284-023-00366-5

Wang, Q., & Chong, T. T. L. (2021). Factor pricing of cryptocurrencies. *North American Journal of Economics and Finance*. https://doi.org/10.1016/j.najef.2020.101348

Wang, S., & Zhu, X. (2021). Evaluation of potential cryptocurrency development ability in terrorist financing. *Policing (Oxford), 15*(4), 2329–2340. https://doi.org/10.1093/police/paab059

Wątorek, M., Drożdż, S., Kwapień, J., Minati, L., Oświęcimka, P., & Stanuszek, M. (2020). *Multiscale characteristics of the emerging global cryptocurrency market*. https://doi.org/10.1016/j.physrep.2020.10.005

Watters, C. (2023). When Criminals abuse the blockchain: Establishing personal jurisdiction in a decentralised environment. *Laws*. https://doi.org/10.3390/laws12020033

Windari, J., Nurzaman, A. F., & Sayeed, R. R. A. (2024). Systematic Literature Review of Blockchain Applications: Insights from India's Case Study. In: *2024 International Conference on Information Management and Technology (ICIMTech)*, (pp. 416–421). https://doi.org/10.1109/ICIMTech63123.2024.10780881

Windsor, D. (2024). *Tax evasion, bribery, and money laundering in Latin America and the Caribbean* (pp. 85–116). https://doi.org/10.4018/979-8-3693-3763-9.ch004

Wood, L. C. N. (2020). Child modern slavery, trafficking and health: A practical review of factors contributing to children's vulnerability and the potential impacts of severe exploitation on health. *BMJ Paediatrics Open*. https://doi.org/10.1136/bmjpo-2018-000327

Wronka, C. (2022). "Cyber-laundering": the change of money laundering in the digital age. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-04-2021-0035

Wronka, C. (2023). Financial crime in the decentralized finance ecosystem: new challenges for compliance. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-09-2021-0218

Wronka, C. (2024). Crypto-asset activities and markets in the European Union: issues, challenges and considerations for regulation, supervision and oversight. *Journal of Banking Regulation*. https://doi.org/10.1057/s41261-023-00217-8

Wu, J., Liu, J., Zhao, Y., & Zheng, Z. (2020). *Analysis of cryptocurrency transactions from a network perspective: An overview*. https://doi.org/10.1016/j.jnca.2021.103139.

Yang, J., Ma, C., Hsiao, S., & Liu, J. (2024). Blockchain governance: a bibliometric study and content analysis. *Technology Analysis & Strategic Management*. https://doi.org/10.1080/09537325.2024.2337347

Zarpala, L., & Casino, F. (2021). A blockchain-based forensic model for financial crime investigation: the embezzlement scenario. *Digital Finance*. https://doi.org/10.1007/s42521-021-00035-5

Zarrin, J., Wen Phang, H., Babu Saheer, L., & Zarrin, B. (2021). Blockchain for decentralization of internet: prospects, trends, and challenges. *Cluster Computing*. https://doi.org/10.1007/s10586-021-03301-8