



Global trends and insights into cryptocurrency-related financial crime

Shaikha Ali Al Naqbi^{a,*}, Haitham Nobanee^{a,b,c,2}, Nejla Ould Daoud Ellili^{a,3}

^a College of Business, Abu Dhabi University, Abu Dhabi, United Arab Emirates

^b Oxford Centre for Islamic Studies, University of Oxford, Oxford, UK

^c Faculty of Humanities & Social Sciences, The University of Liverpool, Liverpool, UK

ARTICLE INFO

JEL classification:

G2
G28
K2
K4
D53
E42

Keywords:

Crypto
Financial crime
Digital currencies
Bibliometric analysis
Blockchain technology

ABSTRACT

This study employs a bibliometric analysis of publications related to cryptocurrency and financial crime, using the Scopus database and VOSviewer. The primary objective was to synthesize literature findings to enhance decision-making processes concerning cryptocurrencies. This analysis covered 424 documents, including book reviews, book chapters, conference papers, and journal articles. Most articles were related to computers and the social sciences. The study identified the most frequently cited documents and the leading nations in terms of citations, document count, and global research partnerships. Cuba had the highest citation count, whereas the United States led in document quantity and international research collaborations. The results suggest the need for robust regulatory frameworks to mitigate cryptocurrency transactions and financial crimes, international collaboration, and partnerships to establish effective regulatory strategies through standardized regulations and comprehensive monitoring systems. Additionally, the financial sector should identify and prevent cryptocurrency attributes that can diminish user anonymity and contribute to increased financial crimes. However, this study only analyzes studies from the Scopus database published between 1996 and 2023, with a focus on cryptocurrency-related financial crimes. Future research could explore the psychology behind cryptocurrency fraud, consumer trust in cryptocurrencies, the classification of cryptocurrency fraud by geography and fintech development, and the impact of regulatory changes on cryptocurrency crime prevention.

Abbreviations: AI, Artificial intelligence; CBDC, Central Bank Digital Currency; MENA, Middle East and North Africa; PRISMA, Preferred Reporting Items for Systematic Reviews and Meta-Analyses; AML, Anti-money laundering; KYC, Know your customer; LGBM, Light Gradient Boosting Machine; FFTs, Fraudulent Financial Transactions; GDPR, General Data Protection Regulation; EU, European Union; FATF, Financial Action Task Force; CTF, Counter-Terrorism Financing; UAE, United Arab Emirates; VC, Virtual Currency; DLT, Distributed Ledger Technologies; NFT, Non-Fungible Tokens; DNN, Deep Neural Network; GNN, Graph Neural Network; BTC, Bitcoin; DCC, Dynamic Conditional Correlation; GRU, Gated Recurrent Unit; ML, Machine Learning; DAP, Decentralized Anonymous Payment.

* Corresponding author.

E-mail address: shaikhaal@hotmail.com (S.A.A. Naqbi).

¹ ORCID: 0009-0008-7804-3090

² ORCID: 0000-0003-4424-5600

³ ORCID: 0000-0003-1032-3965

<https://doi.org/10.1016/j.ribaf.2025.102756>

Received 14 November 2023; Received in revised form 27 August 2024; Accepted 6 January 2025

Available online 10 January 2025

0275-5319/© 2025 Elsevier B.V. All rights are reserved, including those for text and data mining, AI training, and similar technologies.

1. Introduction

Technological advancements, including new financial instruments and tools brought about by cryptocurrencies built on blockchain technology, have provided new opportunities for businesses and individuals. The adoption of cryptocurrencies such as Bitcoin (BTC), Ethereum, and Ripple as digital currencies has had various impacts on the financial sector (Bajaj et al., 2022). These digital assets facilitate the transfer of monetary value beyond financial institutions such as banks (Riley, 2021). Furthermore, they are secured by cryptographic systems that enhance the safety and security of online transactions (Feldman et al., 2021). Advancements in technology and the extensive use of artificial intelligence (AI) to improve the safety of cryptocurrency transactions have led to the adoption of several encryption algorithms currently used for these transactions (Iqbal et al., 2019). Some of these include elliptical curve encryption, public-private key pairs, and hashing functions (Feldman et al., 2021). In this regard, cryptocurrencies, as modern transfers of monetary value, have some benefits that continue to have positive impacts on different financial markets (Riley, 2021). In addition to their safety and security, cryptocurrency transactions are cost-effective due to the absence of transfer fees charged by financial institutions (Rahman and Jin, 2023). They are also highly accessible, requiring only a smartphone or computer with internet access. Accordingly, this has led to growing interest in cryptocurrencies, with the global number of users estimated at 560 million (Bahamazava and Reznik, 2023). Therefore, steady growth in the use of cryptocurrencies could be a red flag that justifies disregarding their potential limitations, especially the likelihood of financial crimes that may hinder financial market stability.

The lack of regulation and monitoring of cryptocurrency transactions by financial institutions and regulators presents a significant financial threat to users of such digital currencies. Such limitations increase users' susceptibility to financial crimes characterized by violations of anti-money laundering (AML) legislation imposed by governments and financial institutions worldwide (Buttigieg et al., 2019). Thus, financial experts contend that the elevated risk of financial crimes associated with the extensive use of cryptocurrencies can cripple global economies by hindering the efficiency of the financial sector. In addition, cryptocurrencies remain largely unregulated in most countries, posing challenges for financial institutions in detecting suspicious transactions (Buttigieg et al., 2019). This lack of regulation consequently fosters an environment conducive to financial crimes, such as money laundering, corruption via fund embezzlement, and bribery (Bahamazava and Reznik, 2023). This study evaluates the conclusions drawn from the existing literature concerning the intersection of cryptocurrency and financial crime. The objective is to ascertain whether contemporary economies should persist in adopting these technologies. This study offers enhanced insights into the use of cryptocurrencies as a preventive measure against financial crimes while underscoring the associated risks that government financial legislation should address.

Modern economies are reluctant to adopt cryptocurrencies as digital currencies despite transaction security because of the risk of money laundering. This warrants thorough investigation, as technological progress, coupled with the escalating threat of financial crimes, can undermine the economy. Without essential interventions to reshape the global financial sector, this predicament could have destabilizing consequences (Al-Tawil, 2023; Feldman, 2021). The imposition of AML legislation governing the safe use of cryptocurrencies as digital currencies is a major step in preventing financial crimes (Al-Tawil, 2023; De Vido, 2020; Li, 2019). However, they are less likely to destabilize the global financial system. Mohan et al. (2023) revealed that financial decision-makers should make informed choices to maximize the benefits of cryptocurrency for economic growth while minimizing the risk of its negative impacts. Since the beginning of research on this topic, researchers have aimed to improve decision-making processes around the effective global adoption of cryptocurrencies. Reynolds and Irwin (2017) and Riley (2021) employed research methodologies to evaluate whether indicators of money laundering within cryptocurrency buyer-seller interactions could be readily identified and mitigated before the worldwide integration of cryptocurrencies. According to Öztürk et al., (2024) and Ali et al. (2021), formulating research questions is essential to conducting a review in a more structured and logical order. Therefore, the following research questions were developed to shape the scope of this bibliometric analysis:

Research Question 1: What are the publication trends, key contributors (including documents, journals, organizations, authors, and countries), most influential publications, and research fronts related to cryptocurrency-related financial crime?

Research Question 2: What are the most common topics and issues in cryptocurrency research, particularly regarding financial crime, and the factors driving this focus?

Research Question 3: What are the emerging areas for future research in combating the risks associated with cryptocurrency-related financial crimes and what innovative strategies can be developed to mitigate these risks effectively?

The bibliometric analysis highlights the steady increase in the number of documents focusing on cryptocurrencies and financial crimes since 2012, whereas the present analysis focuses on studies published since 1996. Of the documents analyzed, 55.4 % were research articles and 34.4 % were conference papers. The remaining reviews, book chapters, conference reviews, and notes on this topic constitute 4.2 %, 3.1 %, 2.4 %, and 0.5 %, respectively. The University of Munster in Germany has the highest number of citations, at 249, although it has published only one paper related to the topic. The top-cited authors include Böhme, Breuker, and Möser, each of whom contributed one document related to cryptocurrencies and financial crimes. The authors garnered 249 citations for each document. Finally, the country with the highest number of citations is Cuba (612), although it produced only one document on the topic between 1996 and 2023. Despite having 311 citations, the United States published 49 documents on this topic during the same period. Accordingly, it has engaged in the highest number of extensive international research collaborations on cryptocurrencies and associated financial crimes.

Bibliometric analyses are important because they can indicate research directions given that they provide a comprehensive overview and classification of research in an area to date. Researchers can benefit from the current bibliometric study by making informed decisions on how to structure their studies and achieve the replicability of their methodologies to emerging themes based on the state of prior research that represents such themes. This study was structured to maximize this advantage by comprehensively illustrating prior research.

The remainder of this article proceeds as follows. [Section 2](#) presents a literature review. [Section 3](#) presents methods. [Section 4](#) introduces the results. [Section 5](#) concludes.

2. Literature review

Over the past 15 years, cryptocurrencies have become more common in financial markets and are well-known for their efficiency in storing and transferring monetary value safely, securely, and transparently. According to [Riley \(2021\)](#) and [Dumchikov et al. \(2022\)](#), cryptocurrencies are digital financial assets secured by blockchain technology and are solely used as a medium via cryptography without intervention from central authorities such as governments or central banks. [Riley \(2021\)](#) reviews cryptocurrency regulations and focuses on China as a nation that has expressed concerns about the unregulated nature of the cryptocurrency industry. By contrast, [Dumchikov et al. \(2022\)](#) discuss a wide range of characteristics associated with countering illegal income from fraudulent cryptocurrency deals. [Feldman et al. \(2021\)](#) identified the role of machine learning algorithms in preventing cryptocurrency-related financial crimes, with a specific focus on abnormal BTC transactions. Cryptocurrencies rely on blockchain technology that is composed of encryption and decryption keys for all online financial transactions. [Feldman et al. \(2021\)](#) further noted that such keys are frequently changed to prevent system attacks and are shared only with the parties involved in a transaction ([Feldman et al., 2021](#)). [Li et al. \(2019\)](#) shared a similar opinion when examining BTC privacy concerns and exploring techniques that could effectively enhance the privacy of digital currency users. Researchers have revealed that the use of blockchain technology leads to a tamper-proof record of cryptocurrency transactions that makes them safe and secure, regardless of the user's geographical location.

Many researchers have noted the high risk of financial crimes related to cryptocurrencies, despite perceptions of the safety of transactions due to the use of blockchain technology. [Utkina et al. \(2023\)](#) described financial crimes resulting from the use of digital currencies and how financial monitoring of transactions can be used to combat such crimes. Researchers have identified money laundering as one of the most common cryptocurrency-related financial crimes. [Buttigieg et al. \(2019\)](#) also identified terrorism financing as another common financial crime related to cryptocurrencies while examining their regulatory frameworks in Malta. [See \(2023\)](#) assessed potential techniques for tackling money laundering in BTC mixers and revealed that financial crimes, such as phishing and Ponzi schemes, are also common with BTC. Finally, [Mohan et al. \(2023\)](#) proposed methods to ensure safety in financial markets, with a particular focus on the cryptocurrency market and financial inclusion. They found that corruption is another common financial crime related to the use of cryptocurrencies and can be effectively addressed by preventing fraudulent transactions. Therefore, the diverse array of financial crimes related to cryptocurrencies signifies the need for immediate intervention to prevent negative economic effects.

Financial crimes identified in prior research have negative economic impacts that can hinder the growth and development of many countries where cryptocurrency use is becoming increasingly common. Al-Tawil and Younies (2021) addressed the important factors hindering AML efforts. They examined the relationship between BTC and financial crimes before revealing that cryptocurrency-related financial crimes increase the risk of a global economic recession. While discussing how to reconcile safety in financial markets and inclusion, [Mohan et al. \(2023\)](#) affirmed that cryptocurrencies may lead to economic inequality in cases of extensive loss of capital by one or more parties. Therefore, they concluded that economic inequality due to losses related to financial crimes may lead to trade wars among nations, which may impede development and increase the risk of a global economic recession. [Haq et al. \(2022\)](#) examined the effectiveness of a state's prohibition of virtual assets in preventing money laundering and affirmed that such assets may lead to an increased risk of financial market collapse in the event of extreme withdrawals of capital from financial markets that rely on cryptocurrency investments and transactions. While illustrating how financial crimes occur during the use of digital currencies, [Utkina et al. \(2023\)](#) noted that some investors may develop a fear of financial losses in such crypto markets, which may, in turn, contribute to negative financial outcomes, such as panic selling of shares and bank runs. Accordingly, the fact that such negative outcomes of cryptocurrency-related financial crimes may become inevitable due to the steady increase in the use of digital currencies highlights the importance of addressing this issue.

2.1. Overall evaluation and gap in the literature

From the literature review, it can be deduced that cryptocurrency use will steadily increase over the next few years. However, this increase may correspondingly increase financial crimes related to cryptocurrency investments and transactions, thereby negatively affecting global economic stability. [De Vido \(2020\)](#) reached this conclusion after analyzing the privacy concerns associated with BTC as one of the most common digital currencies. Implementing innovative strategies to address these crimes can ensure that cryptocurrencies boost the economic growth of many nations. However, the existing literature does not indicate whether any of the proposed strategies for mitigating cryptocurrency-related financial crimes are being implemented in developed or developing economies. In addition, prior studies do not provide statistics on the prevalence of financial crimes related to cryptocurrency use or the instances in which they have been reported. Therefore, there is no practical proof of the extent of economic damage that such crimes cause when they occur.

3. Methods

This study uses bibliometric analysis, integrating both qualitative and quantitative aspects of the research topic. Bibliometric analysis incorporates computer-assisted reviews to identify core research or authors ([Iqbal et al., 2019](#)). The analysis included the relationships between the findings on a given topic, implying that this methodology integrates content and systematic analysis. To

conduct a bibliometric analysis for the present study, performance analysis, visualization, and scientific and bibliographic mapping were combined (Iqbal et al., 2019). Multiple bibliometric analyses were conducted to include citation and keyword analyses, as well as bibliographic coupling, utilizing VOSviewer and Scopus. The bibliometric analysis involved a keyword search within the Scopus database to identify literature on cryptocurrency and money laundering up to 2023.

The search queries encompassed a diverse range of keywords to identify various document types in the Scopus database. Table 1 provides the details of the search queries. The initial query returned 506 documents on cryptocurrencies and financial crimes. These documents included journal articles, conference reviews, papers, and book chapters. To enhance relevance, a screening filter was applied, excluding books and trade journals from the initial search. This refinement yielded 457 documents categorized by source type, year of publication (all years included), subject area, and the number of documents published before the search query date. In addition, the search included only English-language documents, leading to the exclusion of 33 documents. The bibliometric analysis included 424 relevant documents (Fig. 1).

Table 1

Search queries for cryptocurrency and financial crime.

Description	Conditions	Number of Documents
Search query	TITLE-ABS-KEY ((“crypto*” AND “money laund*”) OR (“bitcoin*” AND “money laund*”) OR (“virtual currenc*” AND “money laund*”) OR (“XXXinanceXXX*” AND “money laund*”) OR (“tether*” AND “money laund*”) OR (“digital currenc*” AND “money laund*”) OR (“digital coin*” AND “money laund*”) OR (“XXXinanceXXX*” AND “money laund*”) OR (“namecoin*” AND “money laund*”) OR (“zcash*” AND “money laund*”) OR (“cardano currenc*” AND “money laund*”) OR (“libra currenc*” AND “money laund*”) OR (“polkadot currenc*” AND “money laund*”) OR (“stellar currenc*” AND “money laund*”) OR (“chainlink currenc*” AND “money laund*”) OR (“binance currenc*” AND “money laund*”) OR (“monero currenc*” AND “money laund*”) OR (“ecoin*” AND “money laund*”) OR (“ripple currenc*” AND “money laund*”) OR (“dogecoin*” AND “money laund*”) OR (“petro currenc*” AND “money laund*”) OR (“crypto*” AND “terroris* XXXinance*”) OR (“terroris* XXXinance*”) OR (“virtual currenc*” AND “terroris* XXXinance*”) OR (“XXXinanceXXX*” AND “terroris* XXXinance*”) OR (“tether*” AND “terroris* XXXinance*”) OR (“digital currenc*” AND “terroris* XXXinance*”) OR (“digital coin*” AND “terroris* XXXinance*”) OR (“XXXinanceXXX*” AND “terroris* XXXinance*”) OR (“namecoin*” AND “terroris* XXXinance*”) OR (“zcash*” AND “terroris* XXXinance*”) OR (“cardano currenc*” AND “terroris* XXXinance*”) OR (“libra currenc*” AND “terroris* XXXinance*”) OR (“polkadot currenc*” AND “terroris* XXXinance*”) OR (“stellar currenc*” AND “terroris* XXXinance*”) OR (“chainlink currenc*” AND “terroris* XXXinance*”) OR (“binance currenc*” AND “terroris* XXXinance*”) OR (“monero currenc*” AND “terroris* XXXinance*”) OR (“ecoin*” AND “terroris* XXXinance*”) OR (“ripple currenc*” AND “terroris* XXXinance*”) OR (“dogecoin*” AND “terroris* XXXinance*”) OR (“petro currenc*” AND “terroris* XXXinance*”))	506
Document & Source type	Excludes books, editorials, and trade journals	49
Language	English only	424
Years	1996–2023	
Access	Includes open-access and non-open-access documents	
Query search date	July 2, 2024	
Subject area	All	
Final query after refinement	TITLE-ABS-KEY ((“crypto*” AND “money laund*”) OR (“bitcoin*” AND “money laund*”) OR (“virtual currenc*” AND “money laund*”) OR (“XXXinanceXXX*” AND “money laund*”) OR (“tether*” AND “money laund*”) OR (“digital currenc*” AND “money laund*”) OR (“digital coin*” AND “money laund*”) OR (“XXXinanceXXX*” AND “money laund*”) OR (“namecoin*” AND “money laund*”) OR (“zcash*” AND “money laund*”) OR (“cardano currenc*” AND “money laund*”) OR (“libra currenc*” AND “money laund*”) OR (“polkadot currenc*” AND “money laund*”) OR (“stellar currenc*” AND “money laund*”) OR (“chainlink currenc*” AND “money laund*”) OR (“binance currenc*” AND “money laund*”) OR (“monero currenc*” AND “money laund*”) OR (“ecoin*” AND “money laund*”) OR (“ripple currenc*” AND “money laund*”) OR (“dogecoin*” AND “money laund*”) OR (“petro currenc*” AND “money laund*”) OR (“crypto*” AND “terroris* XXXinance*”) OR (“bitcoin*” AND “terroris* XXXinance*”) OR (“virtual currenc*” AND “terroris* XXXinance*”) OR (“XXXinanceXXX*” AND “terroris* XXXinance*”) OR (“tether*” AND “terroris* XXXinance*”) OR (“digital currenc*” AND “terroris* XXXinance*”) OR (“digital coin*” AND “terroris* XXXinance*”) OR (“XXXinanceXXX*” AND “terroris* XXXinance*”) OR (“namecoin*” AND “terroris* XXXinance*”) OR (“zcash*” AND “terroris* XXXinance*”) OR (“cardano currenc*” AND “terroris* XXXinance*”) OR (“libra currenc*” AND “terroris* XXXinance*”) OR (“polkadot currenc*” AND “terroris* XXXinance*”) OR (“stellar currenc*” AND “terroris* XXXinance*”) OR (“chainlink currenc*” AND “terroris* XXXinance*”) OR (“binance currenc*” AND “terroris* XXXinance*”) OR (“monero currenc*” AND “terroris* XXXinance*”) OR (“ecoin*” AND “terroris* XXXinance*”) OR (“ripple currenc*” AND “terroris* XXXinance*”) OR (“dogecoin*” AND “terroris* XXXinance*”) OR (“petro currenc*” AND “terroris* XXXinance*”)) AND PUBYEAR > 1995 AND PUBYEAR < 2024 AND (EXCLUDE (SRCTYPE, “b”) OR EXCLUDE (SRCTYPE, “d”) AND (LIMIT-TO (LANGUAGE, “English”)))	

Authors' own work.

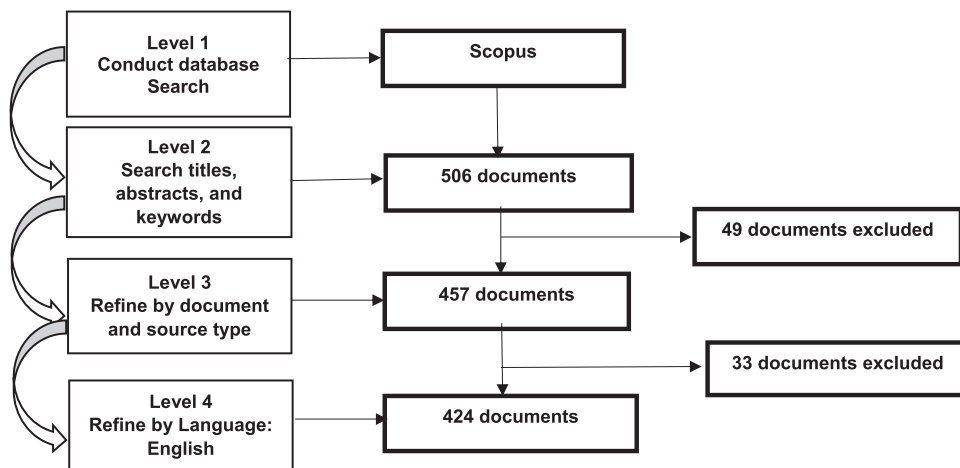


Fig. 1. PRISMA bibliometric study method.
Authors' own work.

4. Empirical results

4.1. Preliminary statistics

Cryptocurrencies are a relatively new form of digital currency invented in January 2009 (Bommer et al., 2023). Therefore, it is expected that most studies on the topic of interest will be published after 2009. Between 1996 and 2023, 424 documents related to cryptocurrencies and financial crimes were identified from the search using the PRISMA methodology, of which 80 % were published between 2012 and 2023, and only 20 % were published between 1996 and 2012. Journal articles were the most commonly published documents on this topic. Finally, most of the documents fell within the disciplines of computer science and social sciences (see Table 2).

4.2. Evolution and growth of crypto and financial crime research

The number of documents published annually on cryptographic and financial crimes was identified using this methodology (Fig. 2). The first publication was in 1996, when three articles related to cryptographic and financial crime prevention were published. However, little research was conducted on this topic over the next two years, with one article each published in 1997 and 1998. The number of published articles increased over the next three years, with an average of three articles published annually. In 2006, the number of articles increased to four, before declining over the next three years to an average of one. Since 2012, the number of articles published on cryptocurrencies and financial crime has increased steadily. This publication trend has gained momentum since 2018, with a significant increase in research on this topic over the past two years. This trend can be attributed to the increase in global interest in the role of cryptocurrencies, along with the heightened adoption of these currencies for investment and financial advancement (Bommer et al., 2023). More than 80 % of this research was published between 2012 and 2024. In 2022, 74 articles on cryptocurrencies and financial crimes were published (Fig. 3). This number was expected to increase to 113 by the year 2023.

Table 2
Summary statistics.

Description	Results
Sample period	1996–2023
Number of sources	279
Number of documents	424
Publications between 1996 and 2012, %	20 %
Publications between 2012 and 2023, %	80 %
Authors	1000
Author's Keywords	118
Countries	73
Journal articles, %	55.4 %
Reviews, %	4.2 %
Conference papers, %	34.4 %
Notes, %	0.5 %
Computer science documents, %	28.5 %
Social science documents, %	18.1 %

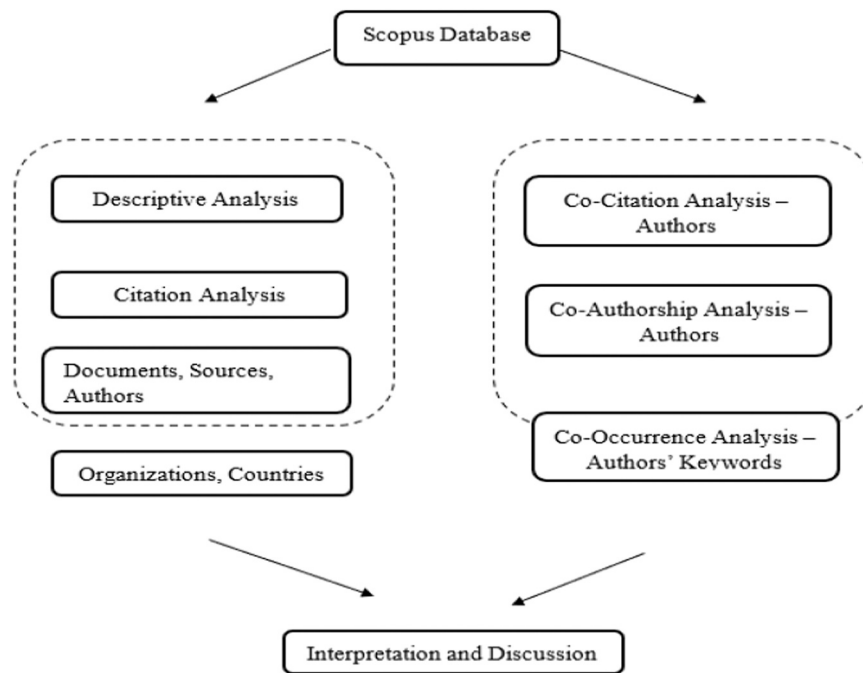


Fig. 2. Bibliometric study methodology.
Authors' own work.

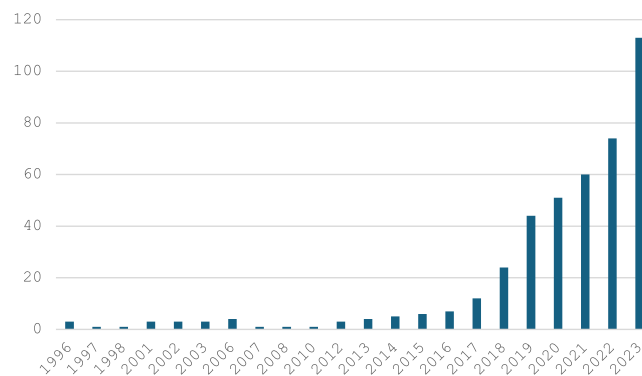


Fig. 3. Publication growth of crypto and financial crime research for all documents.
Authors' own work

4.3. Distribution of documents by type

Since 1996, 55.4 % of the documents related to the topic have been research articles. As of 2023, 34.4 % of the documents were expected to be conference papers. However, only 4.2 %, 3.1 %, 2.4 %, and 0.5 % of these documents were reviews, book chapters, conference reviews, and notes, respectively. The distribution of documents by type is shown in Fig. 4. Published documents on cryptographic and financial crimes can also be categorized based on the domains to which they relate. In this case, 28.5 % of the documents were related to computer science, and 18.1 % were linked to social sciences. In addition, 12.1 % and 12.2 % of documents were related to economics and engineering, respectively. Meanwhile, 6.9 % were linked to mathematics, 6.7 % to business management, 5.5 % to decision science, 2.1 % to physics and astronomy, 1.3 % to materials science, and 1.2 % to energy. Overall, 5.5 % of the documents applied to areas that had a substantial interest in cryptocurrencies and were vulnerable to financial crimes. The distribution of documents by discipline is shown in Fig. 5.

4.4. Most-cited documents

The published documents on cryptographic and financial crimes have received a significant number of citations relative to other

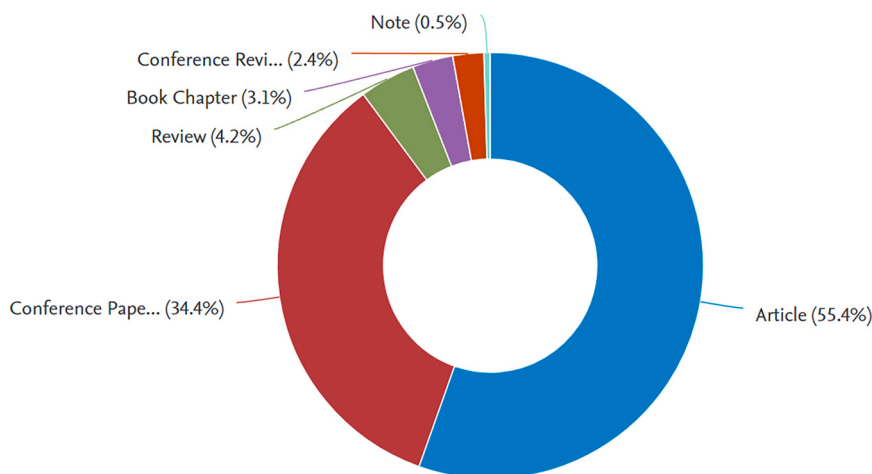


Fig. 4. Distribution of documents by type.
Authors' own work

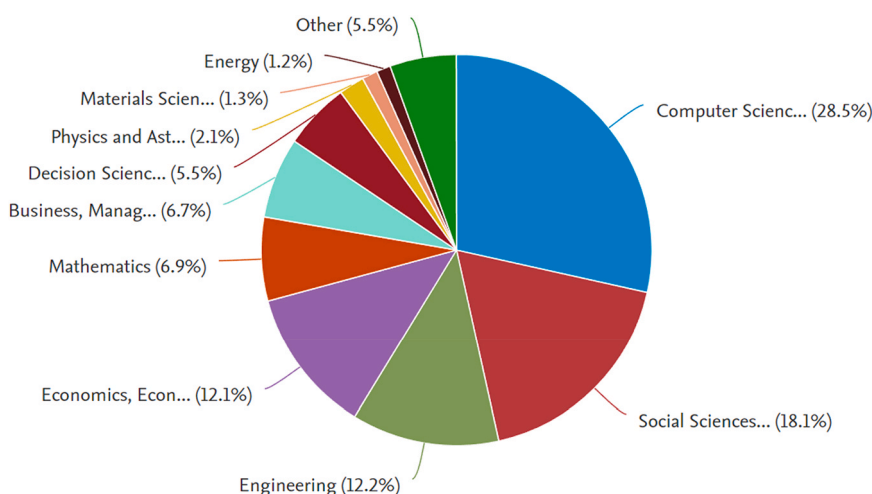


Fig. 5. Distribution of documents by subject area.
Authors' own work

emerging subjects. The most cited document (249 citations) is *An inquiry into money laundering tools in the Bitcoin ecosystem* by Möser et al. (2013), positioned in the first cluster (purple), which delves into cryptocurrency's role in countering financial crimes. This study presents the first systematic account of AML opportunities and their limitations in the BTC ecosystem. The next most-cited is *The ring of gyges: Investigating the future of criminal smart contracts* by Juels et al. (2016), positioned in the first cluster (purple), and *Detection of illicit accounts over the Ethereum blockchain* by Farrugia et al. (2020). *Bitcoin and money laundering: Mining for an effective solution* by Bryans (2014) in the green cluster secured fourth place, and Frankel et al. (1996) followed, with 115 citations of *Indirect discourse proofs: Achieving efficient fair off-line e-cash*. In addition, some of the less-cited documents include those by Lin et al. (2020) with 100 citations, Kethineni and Cao (2020) with 93 citations, Campbell-Verduyn (2018) with 91 citations, Ducas and Wilner (2017) with 89 citations, and McGinn et al. (2016) with 87 citations. The details of the most-cited documents and their respective themes are presented in Table 3 and Fig. 6. Most of the studies were qualitative and empirical, and the top four most-cited documents were published after 2012.

4.5. Top journals

Table 4 and Fig. 7 present the most-cited journals along with the number of documents and citations. The number of papers ranged from 1 to 33, with citations exhibiting substantial variation across journals. *Lecture Notes in Computer Science*, *AI*, and *Bioinformatics* had the highest number of citations (404) with 24 published papers, followed by *Journal of Money Laundering Control* with 400 citations and 33 papers, and *eCrime Researchers' Summit* followed with 249 citations and two papers.

Table 3
Most-cited documents.

Rank	Title	Author(s)	Year	Total Scopus Citations	Source	Methodology
1	An inquiry into money laundering tools in the Bitcoin ecosystem	Möser et al.	2013	249	eCrime Researchers Summit	Empirical analysis
2	The ring of gyges: Investigating the future of criminal smart contracts	Juels et al.	2016	152	Proceedings of the ACM Conference on Computer and Communications Security	Qualitative
3	Detection of illicit accounts over the Ethereum blockchain	Farrugia et al.	2020	142	Expert Systems with Applications	Quantitative
4	Bitcoin and money laundering: Mining for an effective solution	Bryans	2014	118	Indiana Law Journal	Empirical analysis
5	Indirect discourse proofs: Achieving efficient fair off-line e-cash	Frankel et al.	1996	115	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	Qualitative
6	DCAP: A secure and efficient decentralized conditional anonymous payment system based on blockchain	Lin et al.	2020	100	IEEE Transactions on Information Forensics and Security	Qualitative and quantitative
7	The rise in popularity of cryptocurrency and associated criminal activity	Kethineni and Cao	2020	93	International Criminal Justice Review	Systematic content review
8	Bitcoin, crypto-coins, and global anti-money laundering governance	Campbell-Verduyn	2018	91	Crime, Law, and Social Change	Empirical analysis
9	The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada	Ducas and Wilner	2017	89	International Journal	Empirical analysis
10	Visualizing dynamic Bitcoin transaction patterns	McGinn et al.	2016	87	Big Data	Empirical analysis

Authors' work

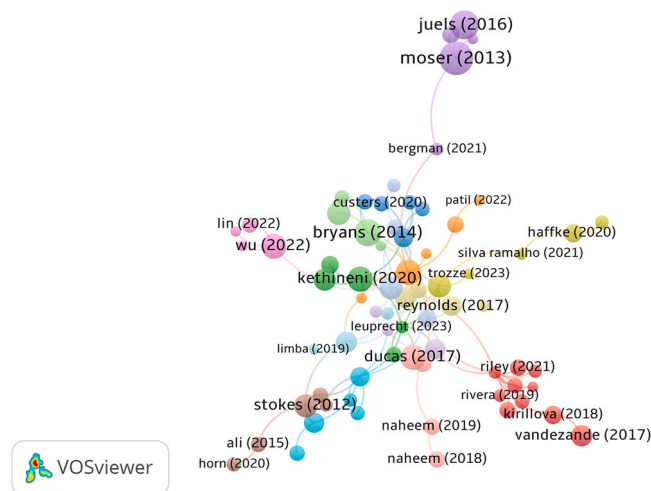


Fig. 6. Most-cited documents.
Authors' elaboration on VOSviewer

4.6. Publications and citations by authors

Table 5 and Fig. 8 present the leading 10 authors by citation count. Böhme, Breuker, and Möser had the highest number of citations (249); followed by Camenisch and Stadler (193); Ellul (184); Wu (154); and Kosba, Shi, and Juels (152).

4.7. Most-cited organizations

The organizations with the highest citation counts are listed in Table 6. The University of Munster (Germany) had the highest number of citations, followed by Cornell Tech (Jacobs Institute), Cornell University, and the University of Maryland in the US. The University of Malta holds fifth place. The top 10 organizations had only one published paper each.

Table 4
Most-cited journals.

Rank	Source	Documents	Citations
1	Lecture Notes in Computer Science, AI, And Bioinformatics	24	404
2	Journal of Money Laundering Control	33	400
3	eCrime Researchers' Summit	2	249
4	Proceedings of the ACM Conference on Computer and Communications Security	4	232
5	Journal Of Financial Crime	12	230
6	Expert Systems with Applications	1	142
7	ACM International Conference Proceeding Series	7	119
8	IEEE Transactions on Information Forensics and Security	2	119
9	Indiana Law Journal	1	118
10	Research in International Business and Finance	2	107

Authors' own work

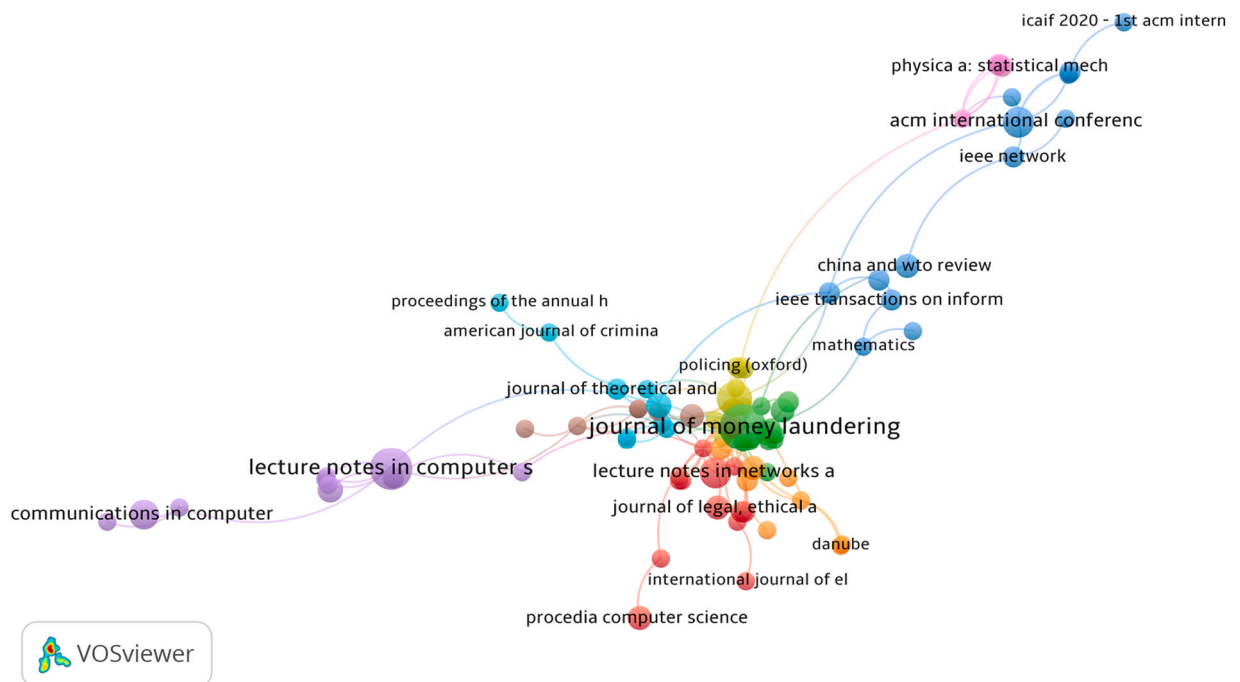


Fig. 7. Top sources for the documents identified in the scopus database.
Authors' elaboration on VOSviewer

Table 5
Most-cited authors.

Rank	Author	Documents	Citations
1	Böhme, R.	1	249
2	Breuker, D.	1	249
3	Möser, M.	1	249
4	Camenisch, J.	3	193
5	Stadler, M.	3	193
6	Ellul, J	2	184
7	Wu, J.	7	154
8	Juels, A.	1	152
9	Kosba, A.	1	152
10	Shi, E.	1	152

Authors' own work

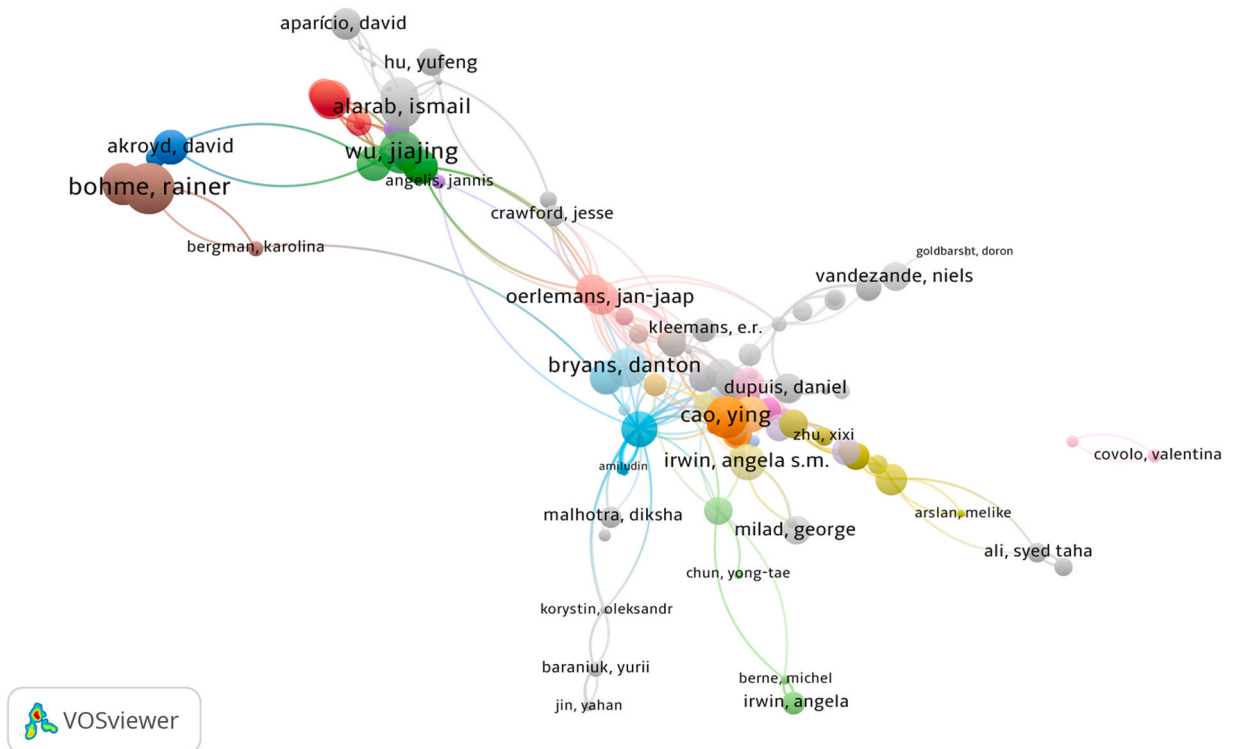


Fig. 8. Most-cited authors.
Authors' own work

Table 6
Most-cited organizations.

Rank	Organization	Country	Documents	Citations
1	University of Munster	Germany	1	249
2	Cornell Tech, Jacobs Institute	United States	1	152
3	Cornell University	United States	1	152
4	University Of Maryland	United States	1	152
5	University of Malta, Tech Centre	Malta	1	142
6	University of Malta, Comp Science	Malta	1	142
7	University of Groningen	Netherlands	1	142
8	Indiana University	United States	1	118
10	North-Eastern University	United States	1	115

Authors' own work

Table 7
Most-cited countries.

Rank	Country	Documents	Citations
1	Cuba	1	612
2	Hungary	3	440
3	Canada	14	337
4	Pakistan	2	313
5	United States	49	311
6	Ireland	3	308
7	Australia	15	245
8	Nigeria	2	201
9	South Korea	13	179
10	Spain	6	178

Authors' own work

4.8. Most-cited countries

Researchers from many countries have published documents on cryptocurrencies and financial crime. The United States had the most, with 49 documents. However, it had 311 citations, fewer than Pakistan, Canada, Hungary, and Cuba, as shown in Table 7. Cuba had the highest number of citations related to crypto and financial crimes. Since 1996, the country has accumulated 612 citations from only one document. Cuba's high citation count can be attributed to the substantial interest among its population in utilizing cryptocurrencies for financial stability and growth. Spain ranked tenth, with 178 citations. However, it has produced only six documents. This number is lower than the 13 published in South Korea, which had 179 citations on this topic. A network map detailing the countries with the highest number of studies, documents, and citations is presented in Fig. 9. Finally, the United States leads the realm of international research collaborations based on the number of documents, followed by Australia with 15 documents. Canada and South Korea also had a considerable number of international research collaborations on this topic.

4.9. Keyword analysis

Table 8 and Fig. 10 present the results of the keyword co-occurrence analysis. This method efficiently identifies related literature and tracks trends. The keywords were divided into several clusters and named according to the most frequent words in each one. "Money Laundering" (146 occurrences) emerged as the most common keyword, presented in the red cluster. This term contained many other keywords such as cryptocurrency, terrorist financing, virtual assets, compliance, banking, financial systems, and so on. Advanced technologies and an increase in cryptocurrencies and other digital assets and channels have led to the growing occurrence of illegal activities, including money laundering and terrorist financing (Lv et al., 2023). Sartori et al. (2022) mention that offenders have found various complex, closely interconnected methods to evade law enforcement and regulators, making it challenging to combat their cryptocurrency use. AbdelAziz and Shalaby (2023) discuss the challenges of virtual currency (VC), noting its ambiguous legal status and difficulties in deducing related crimes. The authors found that while some laws allow cryptocurrencies to be paid, others treat them as crime proceeds and require measures to prevent money laundering and terrorist financing. Thommandru (2023) explored the shift toward electronic banking and the potential for and risk of money laundering through electronic payments, online gambling, and cryptocurrencies.

The next keyword was "Blockchain" (132 occurrences), presented in the blue cluster. Yu et al. (2023) address the challenge of identifying money laundering in blockchain transactions. Samueal and Singh (2023) explore the rise of Central Bank Digital Currencies (CBDCs) due to the impact of cryptocurrencies like BTC on the banking sector, emphasizing the need for strong security measures. Sun et al. (2023) highlight the potential of blockchain technology to address privacy and trust issues in cryptocurrencies. Their study introduces a multichain aggregated identity scheme to allow users to prove their identity across various blockchains while maintaining privacy and ensuring that only regulators can access the user's identity data and walking accounts.

The green "Bitcoin" cluster and "Cryptocurrency," in the red cluster, with 130 and 103 occurrences, respectively, have gained much attention the last several years. Humranan and Supratid (2023) address the challenges of detecting illicit activities in BTC transactions because of their graph complexity and the imbalance between licit and illicit data. Song et al. (2023) examine BTC as a cryptocurrency

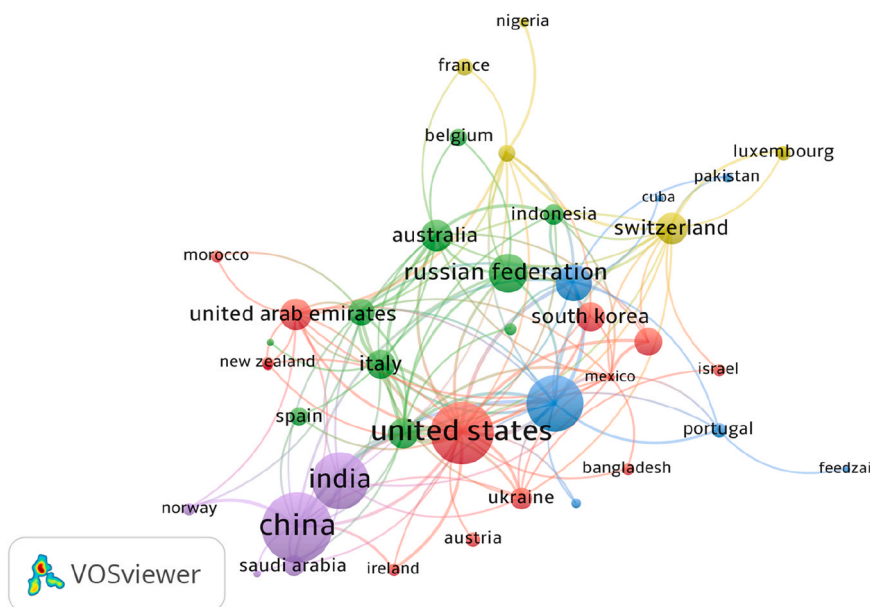


Fig. 9. Top cited countries.
Authors' own work

Table 8
Keyword frequencies.

Rank	Keyword	Occurrences
1	Money Laundering	146
2	Blockchain	132
3	Bitcoin	130
4	Cryptocurrency	103
5	Anti-Money Laundering	72
6	Blockchain	62
7	Laundering	60
8	Crime	58
9	Electronic money	43
10	Cryptography	41
11	Cryptocurrencies	35
12	Anomaly Detection	27
13	Cybercrime	24
14	Finance	24
15	Machine Learning	24

Authors' own work

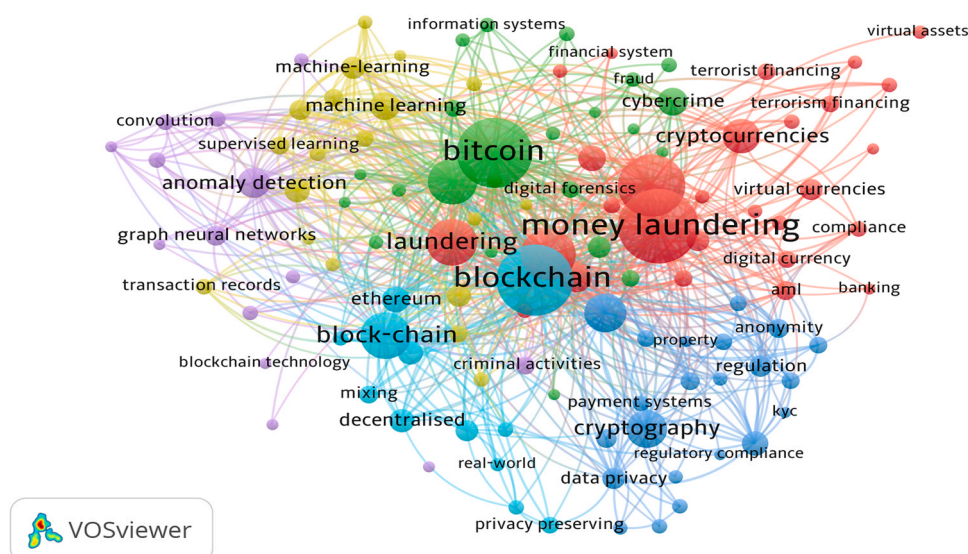


Fig. 10. Visualization of the most frequent keywords. Authors' work

from a terrorism perspective, analyzing its potential for risk hedging and terrorist financing. [Basarud-Din and Abdullah \(2023\)](#) investigate the potential of zakat institutions to accept BTC donations despite their inherent advantages and disadvantages. Their findings suggest strategies for managing BTC zakat donations and addressing related challenges. Finally, [Schullitsch et al. \(2022\)](#) provide an overview of how COVID-19 and the challenges of BTC exchange rates have affected the financial world in terms of money laundering. [Table 9](#) provides more details on the content and other cluster analyses of journal articles.

4.10. Key topics in cryptocurrency research focusing on financial crime

4.10.1. Common topics and issues in cryptocurrency research

The identified articles address various topics and issues related to how digital currencies contribute to financial crimes. Based on an analysis of the scope and findings of the collected studies, the use of cryptocurrencies in money laundering, the anonymity of cryptocurrency money laundering, regulations, ML, blockchain technology, and the role of LGBMs in detecting cryptocurrency-related financial fraud are the most common topics in cryptocurrency research, particularly focusing on financial crimes.

First, the use of cryptocurrencies for money laundering was the most frequent topic in the collected research articles. [Utkina et al. \(2023\)](#) revealed that crypto-tumblers for high-value illicit cryptocurrency transactions play a major role in facilitating money laundering. Financial criminals focus on mixing cryptocurrency funds obtained owing to vulnerabilities in transaction encryption keys and moving them to services where they can be converted into cash while concealing the sources of such vulnerabilities. Second, [Aziz et al. \(2022\)](#) discussed the role of the LGBM in detecting cryptocurrency-related financial fraud in depth and revealed that the LGBM is a

Table 9

Content and cluster analysis of the journal articles.

Cluster	Authors	Main Objective	Main Finding
Anonymity	Reynolds and Irwin (2017)	Assesses BTC anonymity and research potential for tracking illicit transactions by law enforcement.	– Certain exchange services disregard AML regulations and customer identification security standards. This allows tech-savvy criminals to evade identification checks and persist in their transactions. – The paper underscores the need for additional research on criminals' evasion of identity controls to fund illicit endeavors.
	Armstrong and Forde (2003)	Suggests a connection between online criminal activities and online anonymity. The study explores cybercriminals' inclination to use anonymity techniques.	– There must be a new balance between privacy, freedom of speech, and law enforcement.
	Camenisch et al. (1996)	Presents an anonymous digital payment system satisfying all the requirements.	– Proposes a simple protocol for revocation of anonymity that can be used for online or offline payments.
Compliance	Xue et al. (2023)	Presents a novel decentralized anonymous payment (DAP) scheme that supports regulatory compliance.	– Proposes a formal security model and shows that the scheme meets desired security properties; a performance evaluation demonstrates its high efficiency.
	Sun et al. (2022)	Proposes an identification scheme based on Ethereum that complies with know your customer (KYC) policies using Merkle trees and smart contracts.	– This solution supports all public blockchains, necessitating an EVM-compatible blockchain. It surpasses existing solutions that demand additional effort to accommodate new blockchains.
	Pocher and Veneris (2021)	Proposes a techno-legal taxonomy of ways to ensure privacy and transparency in retail CBDs while highlighting cross-sectoral implications.	– Highlights technology's role in legal contexts and the need for regulatory requirements embedded in technology to achieve agreed-upon standards and outcomes.
Privacy	Kanamori et al. (2022)	Analyzes five Japanese banks using privacy-preserving federated learning. Introduces DeepProtect, a novel protocol for privacy-preserving federated learning aimed at detecting fraudulent financial transactions (FFTs) and identifying criminals' bank accounts.	– The proposed federated learning system detected criminals' bank accounts and FFTs before the bank actually froze them.
	Renwick and Gleasure (2021)	Explores privacy attitudes within the Monero cryptocurrency community, which is known for its focus on privacy, decentralization, and values like crypto-anarchism, cypherpunk, or anti-establishment principles using a boundary object perspective.	– Lack of social interest in monitoring routine transactions, despite its clear business and tax collection benefits. – Regulators are content to delay direct engagement, presuming that they can impose regulations once privacy abuse risks are recognized. – Regulators assert that overseeing exceptional transactions is vital to counter broad and easy money laundering.
	De Vido (2020)	Analyzes virtual currencies, specifically BTC, in light of the right to privacy. Based on discussions on the Fifth EU Anti-Money Laundering Directive and the General Data Protection Regulation (GDPR).	– Regulations and laws that incorporate technology knowledge are needed to comply with both the VAML Directive and the GDPR.
	Li et al. (2019)	Examines BTC privacy concerns and explores existing privacy-enhancing techniques in blockchain-based cryptocurrencies and privacy-focused altcoins. Additionally, reviews and compares selected cryptocurrency regulations.	– Owing to BTC privacy limitations, the authors investigate privacy-enhancing techniques, privacy-centric altcoins, methods for monitoring cryptocurrencies, and proposed top-down solutions to strike a balance between privacy and regulatory needs in blockchain-powered cryptocurrencies.
	Al Tawil (2023)	Provides a high-level analysis of how the emerging cryptocurrency sector intersects with AML regulations and risk-based AML diligence systems.	– Key concerns are uncovered in the assessment of the UAE's legislative structure. – A customized strategy is essential, and the Financial Action Task Force (FATF) should set a worldwide standard to facilitate consistent application of AML and Counter-Terrorism Financing (CTF) laws and regulations.
	Draganidis (2023)	Provides an overview of the current view on jurisdictional arbitrage in the general regulatory arbitrage literature and discusses its implications on crypto asset regulation.	– Misinterpretations arise as academics, international entities, and commentators mistakenly employ "regulatory arbitrage" to denote jurisdictional arbitrage, leading to confusion in interpretation. – Commentators often blend jurisdictional conflicts with jurisdictional arbitrage. The remedies for this regulatory concern lie in addressing the root causes of the issue.
			– Demonstrates that cryptocurrency regulation is in its early stages and is characterized by limited
	Bajaj et al. (2022)	Investigates international regulatory approaches using a systematic literature review.	

(continued on next page)

Table 9 (continued)

Cluster	Authors	Main Objective	Main Finding
	Bahamazava and Reznik (2023)	Examines Italian and Russian AML laws to understand their readiness for the new era of laundering based on recent cryptocurrency and blockchain development.	transparency. The pandemic had a minor impact on cryptocurrencies. Macroeconomic uncertainties affect cryptocurrency volatility.
	Sadok and El Maknoui (2021)	Situates VCs in a landscape of regulatory questions to identify the direction and purpose of a possible legal approach in light of recent financial and technological developments.	– Crypto laundering prevention falls behind in both countries, despite the differences in cryptocurrency regulations.
	Fletcher et al. (2021)	Moves beyond the existing legal frameworks by arguing that BTC should be classed as technology and regulated by private technology companies.	– Several VC schemes are impossible to use as private money, competing with sovereign currencies.
	Feinstein and Werbach (2021)	Empirically examines trading activity at several exchanges following key regulatory announcements according to original data on cryptocurrency regulations worldwide.	– Three specific kinds of uses—security tokens, utility tokens, and currency tokens—offer a more realistic look at the risks and potential.
	Riley (2021)	Reviews current trends in crypto regulation, with a particular focus on China. Discusses its current cryptocurrency laws and the new Chinese Cryptography Law.	– Proposes a three-tiered regulatory structure founded on shared community standards and best practices. The initial tier involves the regulation of individual users through BTC companies, constituting the second tier. The third tier, supervised by the World Wide Web Consortium (W3C), governs these BTC companies.
	El Maknoui and Sadok (2021)	Maps the evolving global conversation on VCs and proposes a suitable regulatory framework for VCs in the UAE.	– The models yielded almost null results. Finds no systemic evidence that regulatory measures cause traders to flee or enter the affected jurisdictions, from bespoke licensing regimes to targeted AML and anti-fraud enforcement actions.
	Nikiforova and Nikiforov (2021)	Conducts a comparative analysis of cryptocurrency use with blockchain technology in Russia and other countries. Aims to formulate recommendations for establishing an efficient public administration system in Russia through the extensive adoption of blockchain technology.	– Cryptocurrency regulation differs globally. Legalizing this payment instrument is considered risky, as several countries are concerned about tax evasion, terrorist financing, and other criminal activities.
	Buttigieg et al. (2019)	Examines the framework for regulating crypto assets in Malta, focusing on AML and terrorism financing.	– Recent international developments led to a shift in regulatory attitudes toward VCs.
	Scholl and Bolívar (2019)	Investigates the facets of public value generation that could model smart, fast regulation in the digital age. Examines the potential benefits and challenges of this particular approach to Distributed Ledger Technology (DLT) regulation.	– In the financial market, the state regulation of information technologies must be improved to promote competition, protect investors' rights, and prevent money laundering and fraud.
	Rahman and Jin (2023)	Investigates the future market capitalization of NFTs and provides value orientations for controlling the market in China based on the positive experiences of other countries.	– Malta's framework goes beyond the EU's fifth AML Directive. In addition, the authors argue that the Maltese framework could possibly serve as a model for a more extensive EU regime.
Corruption	van Wegberg et al. (2018)	Investigates BTC money laundering. The authors examine how cybercrime proceeds can be laundered using Dark Web services.	– Identifies seven groups of stakeholders: • Government decision-makers • Regulatory agencies • Fintech companies • Lobbyists • Law firms and legal advisers • DLT developers • DLT firms/licensees.
Cybercrime	Utkina et al. (2023)	Illustrates how virtual assets are used in crime, such as money laundering, and clarifies how financial intelligence (monitoring) can combat money laundering effectively.	– Implementing tax control would increase state revenue and reduce illicit financing endeavors. Introducing tax control within the Chinese NFT market could furnish centralized transaction security and legality assurance, fostering additional growth.
	Dumchikov et al. (2023)	Defines and characterizes the peculiarities of countering illegal income through virtual assets.	– Some of the services examined provided excellent, professional, and well-reviewed services at competitive prices. Other sites accepted BTC without any returns.
Virtual Assets	Haq et al. (2022)	Examines whether a state's prohibition on virtual assets is effective in combating money laundering globally.	– The study demonstrates that financial intelligence (monitoring) of transactions with virtual assets can be effective against money laundering.
	Aziz et al. (2022)	Proposes a method for accurately detecting fraud using a light gradient boosting machine (LGBM). The	– Owing to a lack of legislative regulations regarding "virtual assets," it is difficult to counteract the legalization of criminal proceeds using virtual assets.
			– Excluding virtual assets without meeting the prerequisites can put the financial system at risk and appear to breach legal obligations.
			– Among the three algorithms, LGBM and extreme gradient boosting (XGBoost) provide the highest

(continued on next page)

Table 9 (continued)

Cluster	Authors	Main Objective	Main Finding
Machine learning	Pettersson Ruiz and Angelis (2022)	study compares the LGBM approach to other models, such as random forests and multi-layer perceptrons, which are based on machine learning and soft computing algorithms. Explores the use of machine learning (ML) to reduce the anonymity of cryptocurrency money launderers.	accuracy, with LGBM showing slightly better performance at 98.60 %. – Demonstrates that machine learning tools employed to thwart money laundering within cryptocurrency exchanges are sluggish and warrant optimization. While no individual algorithm achieves absolute efficacy in entirely identifying money laundering transactions, the decision tree algorithm is the most promising option for adoption by cryptocurrency exchanges due to its targeted application.
	Alotibi et al. (2022)	Examines the ability of ML and deep learning techniques to detect money laundering in cryptocurrency.	– Compared to other classifiers, deep neural networks (DNNs) and random forests achieved the highest accuracy rates with promising results for reducing false positives. A random forest classifier achieves an F1-score of 0.99 %, outperforming DNNs.
	Alarab and Prakoowit (2023)	Introduces a method called temporal-GCN that merges long short-term memory and GCN to classify illicit transactions within elliptic data. In contrast to prior research on the extensive BTC transaction graph dataset, this study employs an active learning framework.	– This study found that the temporal-GCN model performed significantly better than the previous experiments based on the same experimental settings.
	Bao et al. (2022)	Identifies the drivers of BTC-based outflows based on the dynamic link between BTC and the local stock market and the correlation structure across regions and analyzes regional differences among investors based on their BTC demand.	– BTC use for investment and illegal purposes is an unregulated global market used to channel funds across countries. – Local financial systems will face pressure due to the increase in dynamic conditional correlation (DCC).
	Mohan et al. (2023)	Demonstrates how to reconcile safety and financial inclusion.	– Demonstrates the superiority of the proposed model for classifying illicit transactions. In addition, using the knowledge distillation framework to fine-tune the system can improve the results.
	Al-Tawil and Younies, 2021	Addresses the most pressing issues facing global AML efforts, including the implications of Brexit and BTC's association with crime.	– Instead of banning BTC trade, a successful regulatory framework can be devised by global financial and IT experts, aided by mining specialists. International collaboration with unified standards can bolster AML/CFT efforts and efficient tax collection through effective regulation and monitoring.
	Kethineni et al. (2018)	Examines whether traditional criminological concepts apply to criminal activities in virtual spaces, factors that contribute to BTC-related offenses, and lessons that can be learned from the current study of BTC-related criminal cases.	– Supports space transition theory, indicating that attributes like flexibility, anonymity, online association, and weak deterrence attract traditional criminals to the internet. This enables cybercriminals to shift between physical and virtual spaces, akin to physical criminals entering the online realm.
	Simser (2015)	Examines the challenges BTC poses to regulators, especially with regard to AML.	– In a peer-to-peer network, BTC relies on complex computer code supported by a robust community. As BTC appears to have a market, it poses unique challenges for the regulators.
	Feldman et al. (2021)	Proposes an algorithm to detect abnormal BTC transactions using ML that may be used for money laundering and counterfeiting.	– The reliability of the classification of abnormal BTC transactions can be determined by using the resampling algorithm in conditions of class imbalance.
	Goldbarsht (2022)	Explores the characteristics of frequent-flier programs and how they contribute to Australian AML laws.	– Frequent-flier programs can serve as a conduit for money laundering because they align with financial system vulnerabilities. Their risk factors, including anonymity, rapid digital transactions, compliance ambiguity, global networks, and lack of oversight, contribute to assessing money laundering risks.
	Sadok and El Maknoui (2021)	Situates VCs in a landscape of regulatory questions that can help guide the direction and purpose of a possible legal approach to recent financial and technological developments.	– VC schemes currently cannot work as private money or be competitive with sovereign currencies because of several features (including their deflationary character and fixed supply). Three specific uses of tokens—security, utility, and currency tokens—offer a more realistic view of their risks and potential.
	Naheem (2018)	Examines how the recent Bit-licensing rules in New York would affect banks and their own risk assessment processes. Discusses the challenges associated with applying financial regulations to software companies instead of financial service companies.	– Virtual and digital currencies will persist, so the results are useful for the banking and regulation industries and economics and banking researchers.

(continued on next page)

Table 9 (continued)

Cluster	Authors	Main Objective	Main Finding
Virtual currencies	Vandezande (2017)	Analyzes how virtual currencies are regulated under EU financial and economic laws, with particular attention to cryptocurrencies.	– Regulatory issues related to this nascent market are currently being debated by legislators worldwide.
	Nikkel (2020)	Describes a subdiscipline of digital forensics that focuses on financial technologies, or fintech.	– Fintech and digital payment investigation require recognition as a new technical subfield of the digital forensics landscape. The digital forensics community is well positioned to provide research for practitioners to enhance investigations in fintech and technical financial activities.
	Dumchikov et al. (2022)	Highlights the need to “legalize” cryptocurrency as a type of money and define when it can be criminalized in Ukraine and worldwide.	– Cryptocurrencies may be essential to the development of information societies and the subject of economic crimes.
	Latimer and Duffy (2019)	Examines digital currency in Australia, including its benefits, problems, risks, and the regulatory response so far.	– Argues that specialist regulation to combat money laundering and terrorism financing while bringing digital currency markets under normal financial regulation is crucial.
	Li et al. (2022)	Examines two CBDC application scenarios: anonymous transactions “using ChebNet-GRU” and real-name transactions in China.	– ChebNet-GRU is the most effective method to detect money laundering behavior. For real-name transactions, traditional ML is better than deep learning.

Authors' own work

cryptocurrency fraud detection algorithm with a high accuracy rating of 98.60 %. The LGBM continuously compares incoming cryptocurrency financial data with an established baseline to determine whether a deviation exists. Therefore, cryptocurrency transaction monitoring and anomaly detection are essential, making it a useful tool for preventing financial fraud associated with digital currencies.

The analysis of the identified articles also identified the anonymity of cryptocurrency money launderers and the lack of regulations as the most common issues related to cryptocurrencies and financial crimes. The anonymity of cryptocurrency money laundering was extensively discussed in the identified articles because it is a major impediment to preventing financial crimes related to cryptocurrency transactions. [Pettersson Ruiz and Angelis \(2022\)](#) stated that cryptocurrency money launderers often find it easier to remain anonymous because the cryptographic nature of transactions promotes the right to privacy, obscuring the amounts and names of the involved parties. However, many studies have confirmed the lack of regulations governing the use of cryptocurrencies and have argued that this explains the high risk of financial crimes posed by such digital financial assets. [Bajaj et al. \(2022\)](#) noted that cryptocurrency regulations are lacking because the use of such digital currencies is still in its early stages. Nonetheless, researchers have warned that the continued lack of cryptocurrency regulations may hinder the development of the legal frameworks necessary to protect investors from massive financial losses, which may be detrimental to the growth of global economies.

4.10.2. Factors driving the focus on cryptocurrency and financial crime research

Two main factors appear to drive the focus of cryptocurrency and financial crime research. The first is the steady growth in the use of cryptocurrencies as digital currencies since their invention in 2009 ([Li et al., 2019](#); [De Vido, 2020](#)). Owing to steady growth in the use of cryptocurrencies, financial markets are concerned about the likelihood of using such digital currencies for various financial crimes such as terrorism financing, money laundering, and Ponzi schemes. Another factor is the unregulated nature of the cryptocurrency industry. Because the cryptocurrency industry is one of the few currently unregulated industries, the transparency of its strategic operations and the ability of governments and financial institutions to protect users from the effects of harmful activities cannot be guaranteed. Accordingly, they are perceived to be at higher risk of financial crimes than regulated industries, indicating the need for more research on how to identify and prevent such crimes.

4.10.3. Discussion and implications of the study

This study employed performance analysis, visualization, and scientific and bibliographic mapping to assess existing research on cryptocurrency and financial crime. The Scopus database was used to identify the publications. The search identified 506 documents that were screened to restrict the sample by publication language, document type, and source. The final list included 424 publications. Only a few publications on cryptocurrencies and financial crimes were published between 1996 and 2010. However, the number of publications steadily increased over the past decade, with 2023 registering the highest number of documents published since 1996. The bibliometric analysis highlighted research articles as the most prevalent document type. Additionally, a considerable portion of the documents pertained to computer science and social sciences. Notably, [Möser et al. \(2013\)](#) had the most cited publications in the realms of crypto and financial crime. Whereas the United States accounted for the majority of documents on this topic, Cuba had the highest number of citations. However, this bibliometric study identified gaps that should be addressed in future research.

The findings identify key contributors and emerging trends, provide stakeholders with valuable insights, and underline the need for robust regulatory frameworks to enhance monitoring mechanisms to mitigate cryptocurrency transactions and financial crimes. As cryptocurrencies are increasingly becoming integrated into the global financial system, the risks of money laundering, terrorist financing, and fraud are also increasing. This study emphasizes the importance of understanding the interactions between cryptocurrency use, financial crime, and international collaborations and partnerships to establish effective regulatory strategies through

standardized regulations and comprehensive monitoring systems.

Furthermore, the research highlights the need for more studies on the impact of fintech and technological change on cryptocurrency-related financial crime and the potential benefits of leveraging advanced technologies such as ML to detect and prevent financial crimes. These areas of investigation are crucial for developing a nuanced understanding of cryptocurrency risks and devising innovative strategies to effectively mitigate these risks.

Overall, this bibliometric analysis provides critical insights that can guide regulators, policymakers, and financial crime professionals in formulating policies and frameworks that balance the benefits of cryptocurrencies with the need to prevent financial crimes. Addressing these issues can secure a financial ecosystem that promotes innovation and mitigates risk.

5. Conclusion

This study employs a bibliometric analysis of publications related to cryptocurrency and financial crime, using the Scopus database

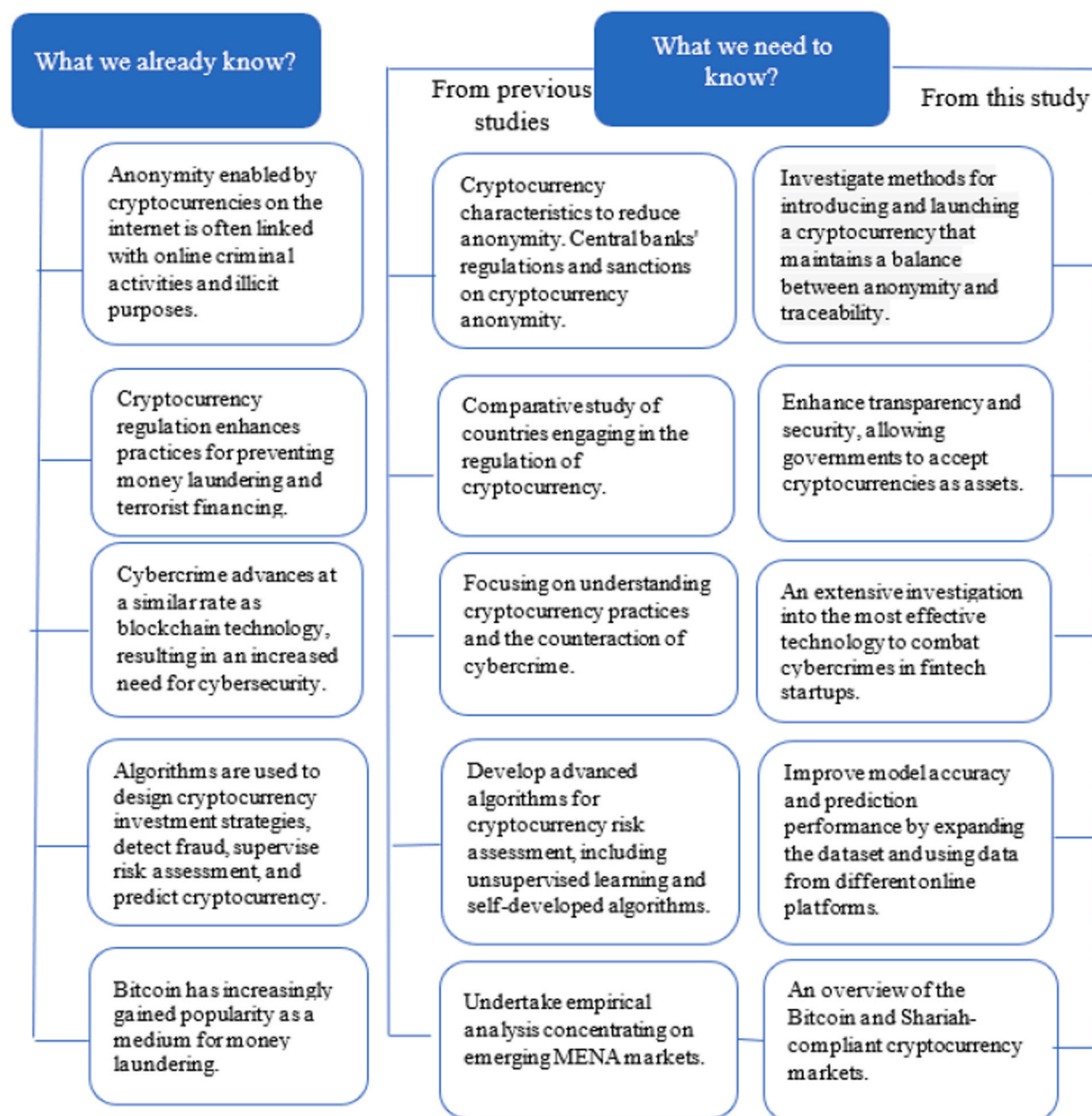


Fig. 11. Summary of future research directions. Authors' own work

and VOSviewer. The primary objective was to synthesize literature findings to enhance decision-making processes concerning cryptocurrencies. In this context, 424 documents, including book reviews, book chapters, conference papers, and journal articles were defined. Most articles were related to computers and the social sciences. The study focuses on publications from 1996 to 2023 and identifies the most frequently cited documents and the leading nations in terms of citations, document count, and global research partnerships. Cuba had the highest citation count, whereas the United States led in document quantity and international research collaborations. The study has important implications, and the results suggest areas for further research, which will be elaborated upon in the limitations and future research section.

5.1. Limitations and future research

This bibliometric study provides valuable insights and information regarding cryptocurrency and financial crime as research domains. However, this method has certain limitations. First, the documents included in this bibliometric study were sourced solely from the Scopus database using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses methodology (Fig. 1). Expanding the scope to include additional databases may yield additional publications on this topic. Second, this study focused only on financial crimes and excluded non-financial scams or fraud. Future research could explore the psychology behind cryptocurrency fraud, consumer trust in cryptocurrency, classification of cryptocurrency fraud by geography and fintech development, and the impact of regulatory changes on cryptocurrency crime prevention.

Furthermore, this study underscores the need for a deeper understanding through future research. These results suggest the need to identify cryptocurrency attributes that could diminish anonymity. Moreover, future studies should examine the regulations and sanctions financial institutions impose on cryptocurrency anonymity (Vandezande, 2017; Naheem, 2018; van Wegberg et al., 2018; Mohan et al., 2023; Lo et al., 2023). Undertaking a comparative analysis of countries engaged in cryptocurrency regulation is imperative. Furthermore, future studies ought to concentrate on comprehending cryptocurrency practices and addressing the cybercrimes associated with these practices (Nikkel, 2020; Nikiforova and Nikiforov, 2021; Kanamori et al., 2022; Ozili, 2022; Pettersson Ruiz and Angelis, 2022). Developing advanced algorithms for cryptocurrency risks and conducting empirical analyses of the utilization of these financial instruments within MENA markets is imperative. Anonymity is the primary risk associated with cryptocurrency use (Kethineni et al., 2018; Latimer and Duffy, 2019; Li et al., 2019; Feldman et al., 2021). Therefore, future research should explore methods to implement and launch these financial tools while balancing anonymity and traceability. Suitable regulations for enhancing transparency and security should also be examined. Additionally, a comprehensive study of the most effective technology for mitigating cybercrime in fintech start-up spaces is essential. Improving the accuracy and predictive capability of cryptocurrency models is also beneficial, and an exploration of BTC and Shariah-compliant cryptocurrency markets will be crucial in the future (Fig. 11).

CRedit authorship contribution statement

Shaikha Ali Al Naqbi: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing. **Haitham Nobanee:** Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization. **Nejla Ould Daoud Ellili:** Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization.

Declaration of Competing Interest

The authors declare that there is no conflict of interest.

Appendix A. Supporting information

Supplementary data associated with this article can be found in the online version at [doi:10.1016/j.ribaf.2025.102756](https://doi.org/10.1016/j.ribaf.2025.102756).

Data availability

Data attached

References

- AbdelAziz, G.M., Shalaby, A., 2023. Legal challenges of cryptocurrency. In: Alareeni, B.A.M., Elgedawy, I. (Eds.), *Artificial Intelligence (AI) and Finance*. Springer Nature Switzerland, Cham, pp. 890–898. https://doi.org/10.1007/978-3-031-39158-3_83.
- Alarab, I., Pragoonwit, S., 2023. Graph-based LSTM for anti-money laundering: experimenting temporal graph convolutional network with Bitcoin data. *Neural Process. Lett.* 55, 1–19. <https://doi.org/10.1007/s11063-022-10904-8>.
- Ali, I., Sultan, P., Aboelmaged, M., 2021. A bibliometric analysis of academic misconduct research in higher education: current status and future research opportunities. *Account. Res.* 28, 372–393. <https://doi.org/10.1080/08989621.2020.1836620>.

- Alotibi, J., et al., 2022. Money laundering detection using machine learning and deep learning. *Int. J. Adv. Comput. Sci. Appl.* 13 (10). <https://doi.org/10.14569/IJACSA.2022.0131087>.
- Al-Tawil, T.N., 2023. Anti-money laundering regulation of cryptocurrency: UAE and global approaches. *J. Money Laund. Control.* <https://doi.org/10.1108/JMLC-07-2022-0109>.
- Al-Tawil, T.N., Younies, H., 2021. The implications of the Brexit from EU and Bitcoin. *J. Money Laund. Control.* 24 (1), 137–149. <https://doi.org/10.1108/JMLC-05-2020-0050>.
- Armstrong, H.L., Forde, P.J., 2003. Internet anonymity practices in computer crime. *Inf. Manag. Comput. Sec.* 11 (5), 209–215. <https://doi.org/10.1108/09685220310500117>.
- Aziz, R.M., et al., 2022. LGBM: a machine learning approach for Ethereum fraud detection. *Int. J. Inf. Technol.* 14, 3321–3331. <https://doi.org/10.1007/s41870-022-00864-6>.
- Bahamazava, K., Reznik, S., 2023. The comparative analysis of regulations in the Italian Republic and the Russian Federation against cryptolaundrying techniques. *J. Money Laund. Control.* 26 (4). <https://doi.org/10.1108/JMLC-01-2022-0016>.
- Bajaj, K., et al., 2022. Risks and regulation of cryptocurrency during pandemic: a systematic literature review. *WSEAS Trans. Environ. Dev.* 18, 642–652. <https://doi.org/10.37394/232015.2022.18.61>.
- Bao, H., et al., 2022. Can Bitcoin help money cross the border: international evidence. *Fin. Res. Lett.* 49. <https://doi.org/10.1016/j.frl.2022.103127>.
- Basarud-Din, S.K., Abdullah, N.S.N., 2023. Can Bitcoin be used for zakat payment? *Int. J. Econ. Manag.* 17 (2). <https://doi.org/10.47836/ijeam.17.2.09>.
- Bommer, W.H., Milevoj, E., Rana, S., 2023. The intention to use cryptocurrency: A meta-analysis of what we know. *Emerging Markets Review* 55, 100962.
- Bryans, D., 2014. Bitcoin and money laundering: mining for an effective solution. *Indiana Law J.* 89, 441.
- Buttigieg, C.P., et al., 2019. Anti-money laundering regulation of crypto assets in Europe's smallest member state. *Law Financ. Mark. Rev.* 13 (4), 211–227. <https://doi.org/10.1080/17521440.2019.1663996>.
- Camenisch, J., et al., 1996. Digital payment systems with passive anonymity-revoking trustees. In: Bertino, E., Kurth, H., Martella, G., Montolivo, E. (Eds.), *Computer Security – ESORICS 96 Lecture Notes in Computer Science*, 1146. Springer, Berlin. (https://doi.org/10.1007/3-540-61770-1_26).
- Campbell-Verduyn, M., 2018. Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime. Law Soc. Change* 69, 283–305. <https://doi.org/10.1007/s10611-017-9756-5>.
- De Vido, S., 2020. Virtual currencies: new challenges to the right to privacy? An assessment under the V AML directive and the GDPR. *Glob. Jurist* 20 (2), 20190045. <https://doi.org/10.1515/gj-2019-0045>.
- Draganidis, S., 2023. Jurisdictional arbitrage: combatting an inevitable by-product of cryptoasset regulation. *J. Financ. Regul. Compliance* 31 (2), 170–185. <https://doi.org/10.1108/JFRC-02-2022-0013>.
- Ducas, E., Wilner, A., 2017. The security and financial implications of blockchain technologies: regulating emerging technologies in Canada. *Int. J. W. J.* 72 (4), 538–562. <https://doi.org/10.1177/0020702017741909>.
- Dumchikov, M., et al., 2022. Digital currency as a subject of economic criminal offenses. *Law State Telecom Rev.* 14 (1), 20–30. <https://doi.org/10.26512/Istr.v14i1.38676>.
- Dumchikov, M., et al., 2023. Peculiarities of countering legalization of criminal income with the help of virtual assets: legislative regulation and practical implementation. *J. Money Laund. Control.* 26 (1), 50–59. <https://doi.org/10.1108/JMLC-12-2021-0135>.
- El Maknoui, M.E.H., Sadok, H., 2021. Regulation of virtual currencies in the United Arab Emirates: accounting for the emerging public/private distinction. *Dev. Stud. Res.* 8 (1), 346–355. <https://doi.org/10.1080/21665095.2021.1980413>.
- Farrugia, S., et al., 2020. Detection of illicit accounts over the Ethereum blockchain. *Expert Syst. Appl.* 150, 113318. <https://doi.org/10.1016/j.eswa.2020.113318>.
- Feinstein, B.D., Werbach, K., 2021. The impact of cryptocurrency regulation on trading markets. *J. Financ. Regul.* 7 (1), 48–99. <https://doi.org/10.1093/jfr/fjab003>.
- Feldman, E.V., et al., 2021. Bitcoin abnormal transaction detection based on machine learning. In: van der Aalst, W.M.P., Batagelj, V., Buzmakov, A., et al. (Eds.), *Recent Trends in Analysis of Images, Social Networks and Texts*. Springer, Cham, pp. 205–215.
- Fletcher, E., et al., 2021. Countering money laundering and terrorist financing: a case for Bitcoin regulation. *Res. Int. Bus. Fin.* 56. <https://doi.org/10.1016/j.ribaf.2021.101387>.
- Frankel, Y., et al., 1996. Indirect discourse proofs: achieving efficient fair off-line e-cash. In: Kim, K., Matsumoto, T. (Eds.), *Advances in Cryptology—ASIACRYPT'96*. Springer, Berlin, pp. 286–300.
- Goldbarsht, D., 2022. Virtual currencies as a quasi-payment tool: the case of frequent-flier programs and money laundering. *J. Money Laund. Control.* 25 (1), 150–164. <https://doi.org/10.1108/JMLC-11-2020-0127>.
- Hag, M.Z., et al., 2022. Could banning virtual assets be a breach of the doctrine of legitimate expectation? *J. Money Laund. Control.* 25 (4), 719–729. <https://doi.org/10.1108/JMLC-07-2021-0077>.
- Humranan, P., Supratid, S., 2023. A study on GCN using focal loss on class-imbalanced Bitcoin transaction for anti-money laundering detection. 2023 International Electrical Engineering Congress (iEECON). IEEE, pp. 101–104. <https://doi.org/10.1109/IEEECON56657.2023.10126580>.
- Iqbal, W., et al., 2019. A bibliometric analysis of publications in computer networking research. *Scientometrics* 119, 1121–1155. <https://doi.org/10.1007/s11192-019-03086-z>.
- Juels, A., et al., 2016. The ring of Gyges: Investigating the future of criminal smart contracts. In: Weippl, E., Katzenbeisser, S. (Eds.), 2016 ACM SIGSAC Conference on Computer and Communications Security. Association for Computing Machinery, New York, NY, pp. 283–295.
- Kanamori, S., et al., 2022. Privacy-preserving federated learning for detecting fraudulent financial transactions in Japanese banks. *J. Inf. Process.* 30, 789–795. <https://doi.org/10.2197/ipsjip.30.789>.
- Kethineni, S., et al., 2018. Use of Bitcoin in darknet markets: examining facilitative factors on Bitcoin-related crimes. *Am. J. Crim. Justice* 43, 141–157. <https://doi.org/10.1007/s12103-017-9394-6>.
- Kethineni, S., Cao, Y., 2020. The rise in popularity of cryptocurrency and associated criminal activity. *International Criminal Justice Review* 30 (3), 325–344.
- Latimer, P., Duffy, M., 2019. Deconstructing digital currency and its risks: why ASIC must rise to the regulatory challenge. *Fed. Law Rev.* 47 (1), 121–150. <https://doi.org/10.1177/0067205X18816237>.
- Li, Y., et al., 2019. Toward privacy and regulation in blockchain-based cryptocurrencies. *IEEE Netw.* 33 (5), 111–117. <https://doi.org/10.1109/MNET.2019.1800271>.
- Li, Z., et al., 2022. Transactional network analysis and money laundering behavior identification of Central Bank digital currency of China. *J. Soc. Comput.* 3 (3), 219–230. <https://doi.org/10.23919/JSC.2022.0011>.
- Lo, W.W., et al., 2023. Inspection-L: self-supervised GNN node embeddings for money laundering detection in bitcoin. *Appl. Intell.* 53, 19406–19417. <https://doi.org/10.1007/s10489-023-04504-9>.
- Lv, W., et al., 2023. Detection of money laundering address over the Ethereum blockchain. in: 2023 5th International Conference on Frontiers Technology of Information and Computer (ICFTIC). IEEE, pp. 866–869. <https://doi.org/10.1109/IJCNN54540.2023.10191217>.
- McGinn, D., et al., 2016. Visualizing dynamic Bitcoin transaction patterns. *Big Data* 4 (2), 109–119. <https://doi.org/10.1089/big.2015.0056>.
- Mohan, A., et al., 2023. Improving anti-money laundering in Bitcoin using evolving graph convolutions and deep neural decision forest. *Data Technol. Appl.* 57 (3), 313–329. <https://doi.org/10.1108/DTA-06-2021-0167>.
- Möser, M., et al., 2013. An inquiry into money laundering tools in the Bitcoin ecosystem, in: 2013 APWG eCrime Researchers Summit. IEEE, San Francisco, CA, USA, 1–14. <https://doi.org/10.1109/eCRS.2013.6805780>.
- Naheem, M.A., 2018. Regulating virtual currencies – the challenges of applying fiat currency laws to digital technology services. *J. Financ. Crime* 25 (2), 562–575. <https://doi.org/10.1108/JFC-08-2016-0055>.
- Nikiforova, V.D., Nikiforov, A.A., 2021. State regulation of blockchain technology in the sphere of payments and financial services. In: Popkova, E.G., Ostrovskaya, V. N., Bogoviz, A.V. (Eds.), *Socio-economic Systems: Paradigms for the Future*. Studies in Systems, Decision and Control, 314. Springer, Cham. https://doi.org/10.1007/978-3-030-56433-9_9.

- Nikkel, B., 2020. Fintech forensics: criminal investigation and digital evidence in financial technologies. *Forensic Sci. Int. Digit. Investig.* 33, 200908. <https://doi.org/10.1016/j.fsi.2020.200908>.
- Ozili, P.K., 2022. Central bank digital currency in India: the case for a digital rupee. *Compét. Advant., Strategy Innov. Afr.: Issues Appl.* (<https://ssrn.com/abstract=4238138>) (accessed 4 September 2023).
- Öztürk, O., et al., 2024. How to design bibliometric research: an overview and a framework proposal. *Rev. Manag. Sci.* <https://doi.org/10.1007/s11846-024-00738-0>.
- Pettersson Ruiz, E., Angelis, J., 2022. Combating money laundering with machine learning—applicability of supervised-learning algorithms at cryptocurrency exchanges. *J. Money Laund. Control.* 25 (4), 766–778. <https://doi.org/10.1108/JMLC-09-2021-0106>.
- Pocher, N., Veneris, A., 2021. Privacy and transparency in CBDCS: a regulation-by-design aml/cft scheme. *IEEE Trans. Netw. Serv. Manag.* 19 (2), 1776–1788. <https://doi.org/10.1109/TNSM.2021.3136984>.
- Rahman, J., Jin, Y., 2023. The control of tax corruption: evidence from nonfungible token market in China. *J. Money Laund. Control.* <https://doi.org/10.1108/JMLC-01-2023-0005>.
- Renwick, R., Gleasure, R., 2021. Those who control the code control the rules: how different perspectives of privacy are being written into the code of blockchain systems. *J. Inf. Technol.* 36 (1), 16–38. <https://doi.org/10.1177/0268396220944406>.
- Reynolds, P., Irwin, A.S.M., 2017. Tracking digital footprints: anonymity within the Bitcoin system. *J. Money Laund. Control.* 20 (2), 172–189. <https://doi.org/10.1108/JMLC-07-2016-0027>.
- Riley, J., 2021. The current status of cryptocurrency regulation in China and its effect around the world. *China WTO Rev.* 7 (1), 135–152. <https://doi.org/10.14330/cwr.2021.7.1.06>.
- Sadok, H., El Maknoui, M.E.H., 2021. The regulation of virtual currencies in comparative perspective: new private money or niche technological innovation? *J. Money Laund. Control.* 24 (4), 712–724. <https://doi.org/10.1108/JMLC-09-2020-0101>.
- Samuel, S., Singh, R.R., 2023. Blockchain in banking: a study on central bank digital currency. *Multidiscip. Sci. J.* 5. <https://doi.org/10.31893/MULTISCIENCE.2023SS0302>.
- Sartori, M., et al., 2022. The illicit use of cryptocurrency on the darknet by cyber criminals to evade authorities. *Conference on Innovative Technologies in Intelligent Systems and Industrial Applications*. Springer Nature Switzerland, Cham, pp. 449–459. https://doi.org/10.1007/978-3-031-29078-7_39.
- Scholl, H.J., Bolívar, M.P.R., 2019. Regulation as both enabler of technology use and global competitive tool: the Gibraltar case. *Gov. Inf. Q.* 36 (3), 601–613. <https://doi.org/10.1016/j.giq.2019.05.003>.
- Schullitsch, M., et al., 2022. Bitcoin here, Bitcoin there, Bitcoin everywhere nonetheless where are the (negative) interest rates?. In: *AIP Conference Proceedings*, 2522 AIP Publishing. <https://doi.org/10.1063/5.0101120>.
- See, K., 2023. The Satoshi laundromat: a review on the money laundering open door of Bitcoin mixers. *J. Financ. Crime.* <https://doi.org/10.1108/JFC-11-2022-0269>.
- Simser, J., 2015. Bitcoin and modern alchemy: in code we trust. *J. Financ. Crime.* 22 (2), 156–169. <https://doi.org/10.1108/JFC-11-2013-0067>.
- Song, Y., et al., 2023. Cryptocurrency technology revolution: are Bitcoin prices and terrorist attacks related? *Financ. Innov.* 9 (1), 29. <https://doi.org/10.1186/s40854-022-00445-3>.
- Sun, N., et al., 2022. A privacy-preserving KYC-compliant identity scheme for accounts on all public blockchains. *Sustainability* 14 (21). <https://doi.org/10.3390/su142114584>.
- Sun, N., et al., 2023. A universal privacy-preserving multi-blockchain aggregated identity scheme. *Appl. Sci.* 13 (6), 3806. <https://doi.org/10.3390/app13063806>.
- Thommandru, A., 2023. Smurfing in electronic banking: a legal investigation of the potential for transnational money laundering. *Int. J. Leg. Inf.* 51 (1), 69–76. <https://doi.org/10.1017/jli.2023.13>.
- Utkina, M., et al., 2023. Financial intelligence (monitoring) of the transactions with virtual assets: new legislation and best practices of foreign countries. *J. Money Laund. Control.* 26 (2), 349–360. <https://doi.org/10.1108/JMLC-12-2021-0136>.
- van Wegberg, R., et al., 2018. Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using Bitcoin. *J. Financ. Crime.* 25 (2), 419–435. <https://doi.org/10.1108/JFC-11-2016-0067>.
- Vandezande, N., 2017. Virtual currencies under EU anti-money laundering law. *Comput. Law Sec. Rev.* 33 (3), 341–353. <https://doi.org/10.1016/j.clsr.2017.03.011>.
- Xue, L., et al., 2023. Enabling regulatory compliance and enforcement in decentralized anonymous payment. *IEEE Trans. Depend. Sec. Comput.* 20 (2), 931–943. <https://doi.org/10.1109/TDSC.2022.3144991>.
- Yu, L., et al., 2023. Who are the money launderers? Money laundering detection on blockchain via mutual learning-based graph neural network. *2023 International Joint Conference on Neural Networks (IJCNN)*. IEEE, pp. 1–8. <https://doi.org/10.1109/IJCNN54540.2023.10191217>.

Shaikhah Ali Al Naqbi is a DBA candidate at the College of Business Administration, Abu Dhabi University, United Arab Emirates. She holds a master's in finance from Hult International Business School, USA. She is certified by MIT in leadership, strategy, artificial intelligence, innovation, and technology. In addition, she is certified by IMD in sustainability and by Harvard Business School in financial accounting. Her research interests are in the areas of FinTech, financial crimes, strategy, leadership, and digitalization

Haitham Nobanee is a professor of finance working at Abu Dhabi University, UAE. An honorary professor at the University of Liverpool, U.K., and a visiting research professor at the University of Oxford, U.K. He received his doctorate from the University of Manchester. He is also serving the academic community as an editor (*Arab Gulf Journal of Scientific Research-Emerald*), associate editor (*International Review of Financial Analysis- Elsevier*) & (*Heliyon- Elsevier*), guest editor (*International Review of Economic & Finance- Elsevier*) & (*Big Data Journal*), member of the editorial board (*Financial Innovation- Springer*) and reviewer of various international refereed journals.

Nejla Ould Daoud Ellili is currently a Professor of Finance at Abu Dhabi University, United Arab Emirates. She received her Ph.D. degree in Finance from Institut Supérieur de Gestion, Tunis, Tunisia. Her research and teaching activities have been in the areas of corporate finance, corporate governance, corporate disclosure, and sustainability. Her works have been published in *Renewable and Sustainable Energy Reviews*, *Corporate Governance: The International Journal of Business in Society*, *Corporate Social Responsibility and Environmental Management*, *Review of Managerial Science*, *International Review of Economics and Finance*, and *Journal of Sustainable Finance and Investment*, among others.