Cryptocurrency and financial crimes: A bibliometric analysis and future research agenda

Sabuj Saha, Ahmed Rizvan Hasan, Alvi Mahmud, Nujhat Ahmed, Nahida Parvin, Hemal Karmakar

Abstract The use of cryptocurrency for financial crimes has increased in recent years because of its decentralized and anonymous nature. This study extracted scholarly articles from the Scopus database and adopted bibliographic and content analysis to review financial fraud research in cryptocurrency. In addition, this study discussed the top ten cryptocurrency scams, potential reasons for falling into those traps, and associated theories to explore scammers’ behavior and outlined comprehensive future research guidelines for a safer financial world. Since 2018, the publication trend of revealing cryptocurrency frauds has gained momentum, and research on this topic has increased significantly in the last two years. The USA is the most significant contributor to cryptocurrency scam research. We found that both developed and developing countries are fairly concerned about combating crypto fraudsters even though there are no regulated guidelines across the countries. The research potential has shifted from malware, bitcoin, and blockchain to fintech-based crimes such as money laundering, pump-and-dump schemes, and phishing. We observed that ICO fraud, money laundering, Ponzi schemes, phishing, darknet market transactions, ransomware, and pumps and dumps are some of the predominant crimes in crypto and that investor overconfidence, speculative expectations, low barriers to entry, decentralization, and anonymity are the primary reasons for crimes in cryptocurrency. This study suggests studying the socioeconomic impacts of cryptocurrencies, the necessity for standardized global regulation, and the integration of interdisciplinary research. Future research should emphasize exploring the innovation cycle in cryptocurrency assets, understanding cybercrime dynamics, guarding against crypto market manipulation, and developing automated scam prevention.

Keywords: crypto, frauds, scams, future directions

1. Introduction

Termed “Wild Wild West”, cryptocurrency is a digital asset that operates independently of government or bank oversight, in contrast to government-issued fiat money. It relies on decentralized technology, such as blockchain, to maintain its security and authenticity without being overseen by any trusted third party or regulatory body (Bailey et al., 2021). Instead of relying on a central authority such as traditional currencies, cryptocurrencies use an encrypted network to execute, verify, and record transactions. This decentralized approach enables high levels of anonymity and privacy in transactions that have led to cryptocurrency being the heaven for financial crimes such as cybercrime, money laundering, and sex and drug trafficking. According to a new analysis from the Federal Trade Commission, consumers reported losing over $1 billion to fraud involving cryptocurrencies from January 2021 through March 2022. Cryptocurrency is rapidly emerging as the payment of choice for scammers, with a staggering one in every four dollars lost to fraud being paid in cryptocurrency. It is concerning that unauthentic cryptocurrency investment opportunities have caused significant consumer losses. According to the FTC’s latest Consumer Protection Data Spotlight, these losses totaled $575 million since January 2021. Scammers often use urgency and scarcity tactics to compel individuals to invest hastily and obtain quick-reach schemes; however, numerous fraudulent operations purport offering investors significant returns, only for the latter to report losing their entire investment.

The rise of cryptocurrencies is attributed to various factors, including their potential for high returns on investment, the appeal of the underlying blockchain technology, the desire for financial privacy, and the ease of cross-border transactions. These factors contribute to the growing interest and investment in cryptocurrencies globally (Sanz-Bas et al., 2021). Inherent features of cryptocurrency often facilitate the successful scamming of victims by scammers. Anonymity and pseudonymity, which are alluring features of cryptocurrency, facilitate cryptocurrency-related scams. Koerhuis et al. (2020) have discussed privacy-oriented cryptocurrencies, i.e., Monero & Verge, with features such as being nonpublic.
Blockchain, hidden addresses, and vague transaction amounts. While legitimate users prefer such privacy, criminals also utilize these features to conceal traces of cryptocurrency fraud. Cryptocurrencies are founded on blockchain technology, which is claimed to be immune to hacking and change. Castonguay & Stein Smith (2020) examined cases in which the blockchain was prone to malefices and fraud, as the criminals were able to hack information directly off the blockchain. Cryptocurrency global outreach and a lack of uniformity in global regulations regarding such outreach add fuel to fraudulent activities. Geographical barriers do not constrain crypto fraudsters, while multiple jurisdictions follow different rules and regulations regarding cryptocurrency. Teichmann Falkor (2020) depicted how many cryptocurrency scams happen by transferring funds across different legal jurisdictions to avoid being caught. Kien & Binh (2021), Kutera (2022), and Wronka (2021) discussed how the global reach of cryptocurrency and the lack of international regulation aid fraudsters in committing more crimes. A lack of customer awareness also contributes to cryptocurrency schemes such as phishing, fake initial coin offerings, pump-and-dump, etc. Chergarova et al. (2022) explained the sophisticated methods scammers apply to lure customers using fake profiles on social media, such as Facebook, Telegram, and WhatsApp, to invest in fake crypto wallets or pump-and-dump schemes.

Cryptocurrency frauds have a far more far-reaching impact than is assumed. These frauds result in substantial financial losses for individuals and institutions and undermine trust in the cryptocurrency market (Broadhead, 2018). Such erosion of trust can deter future investments and innovations in the digital currency sphere. Moreover, these frauds expose the vulnerabilities of unregulated digital currency markets, highlighting the need for more robust security measures and regulatory frameworks to protect investors and maintain market integrity (Gandal et al., 2018). These measures are critical in combating the rise of cryptocurrency-related criminal activities and maintaining confidence in digital currencies. Over the last decade, a wide range of crimes have emerged in the crypto ecosystem. Among these crimes are money laundering, pyramid (Ponzi) schemes, initial coin offering (ICO) fraud, phishing, ransomware, malware, pumps and dumps, and darknet market transactions (Almaqableh et al., 2023; Alyami et al., 2023; Chergarova et al., 2022; Trozze et al., 2022). While lawmakers worldwide are trying to establish regulations to safeguard investors from fraudsters and scammers, progress could be faster and more promising. The FTX fallout is an excellent example of a lack of transparency and accountability that regulations have yet to address. Various government agencies worldwide have shown concern over the increase in crypto-crimes and loss to investors (Trozze et al., 2022). Currently, the cryptocurrency market capitalization is above $1.5T, and with more new currencies entering the market, it is expected to grow further. This expansion could give rise to new types of crimes or the escalation of existing crimes, posing threats to investors and users. Beyond individual financial risks, Crypto has also become a concern in geopolitics. Governments in countries such as Venezuela, Iran, Russia, and North Korea are trying to issue their currencies to avoid sanctions and perform cross-border fund transfers (Kethineni & Cao, 2020). All these growing concerns over Crypto have attracted the attention of academics and researchers, which explains the growth of research on cryptocurrency crimes. This research considers both a bibliometric review and content analysis to provide a wide range of broader perspectives on an array of financial crime optics in cryptocurrency mechanisms. To understand the spectrum between cryptocurrency-related fraud and crimes, we review the literature in the following questions.

- What are the fundamental academic research interests related to cryptocurrency and financial crimes considering key topics, influential authors, significant affiliations, global research trends, and geographical circumstances? (Research Question 1)

- What are the top ten cryptocurrency crimes discussed in the literature? What are the reasons behind those cryptocurrency crimes that have emerged in recent years? What are the underlying theories to explain this increase in cryptocurrency crimes? (Research Question 2)

- What is the future research direction regarding opportunities, challenges, and threats of cryptocurrency crimes? What potential future directions can mitigate these risks? (Research Question 3)

Since 2018, the publication trend of revealing cryptocurrency frauds has gained momentum, and the number of publications will increase exponentially by 2022 and 2023. Universities from the UK and Australia published most of their research on cryptocurrency scams. The USA is the most significant contributor to cryptocurrency scam research, with ten publications. Although developing countries have contributed much more to research on crypto scams, publications from developed countries have been cited significantly. Many collaborative approaches have been found between the USA and the UK, between the USA and China, and between Australia and Canada. In 2018–2023, the emphasis shifted from malware, bitcoin, and blockchain to fintech-based crimes such as money laundering, pump-and-dump schemes, and phishing. Cryptocurrency research has focused on the facets of crypto-crimes, such as money laundering, cybersecurity, digital forensics, and regulation, as evidenced by thematic maps. These included using cryptocurrencies in illicit activities, regulatory challenges, the societal impacts of technological innovations such as blockchain, and the difficulties in tracking the cryptocurrency footprint in illegal activities. ICO fraud, money laundering, Ponzi schemes, phishing, darknet market transactions, ransomware, pumps and dumps, exchange scams, and corruption are some of the predominant crimes in crypto. Investor overconfidence, speculative expectations, low barriers to entry, decentralization, and anonymity are the primary reasons for crimes in cryptocurrency. The study also suggests specific research questions centered around...
monitoring illegal crypto activities, regulatory frameworks, fraud identification, societal effects of tech innovation, and developing new forensic tools.

This study has made several significant contributions to the scholarly literature in three distinct ways. First, it sheds light on the critical geographic reasons, journals, academicians, institutions, publishers, and research areas that are receiving increasing attention for evolving crimes in cryptocurrency. This will help potential researchers develop new innovative ideas and streamline research development. Second, the study provides a comprehensive review of the nature of cryptocurrency crimes, possible reasons, and theories explaining the underlying factors that facilitate illicit behavior in cryptocurrency. This will enable users and market participants to better understand the interplay of different crime patterns with cryptocurrencies. Last, the study covers essential points for policymakers, users, regulators, and governments to openly discuss challenges and opportunities to make digital currency safer and guide the future direction to mitigate potential risks coming from cryptocurrency. This study proposes a research agenda focused on addressing challenges related to ransomware attacks, blockchain-based reporting schemes, and cryptocurrencies in illegal activities. It emphasizes the need for improved user awareness, enhanced security, and anonymity for whistleblowers and for investigating cryptocurrencies’ role in money laundering and fundraising fraud.

2. Methodology

The Scopus database was used to collect all past academic research papers regarding financial crimes on cryptocurrency. Agrawal et al. (2023) stated that the Scopus database is a reliable option for conducting research in the investigative field. With a vast collection of abstracts and citations from peer-reviewed research articles worldwide, it is among the largest databases available. In addition, there was a significant overlap of approximately 84% between the Web of Science and Scopus databases. For our current research area, Scopus seems to be a better fit because it provides a comprehensive understanding of cryptocurrency fraud in the past and helps in identifying influential works performed over the years. This study extracted past scholarly articles from the Scopus database on Dec 10, 2023.

The review methodology was designed and is presented in Figure 1 following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) statement, description, and extension guidelines. In the review process, a five-step process was followed: a) Identify the research questions. b) Identify search databases and keyword selections. c) Screening out relevant documents, d) performing bibliometric and content analysis, e) systematic analysis of the results. As this study concentrates on two main keywords, cryptocurrency and financial crime, we employed the following search string to identify the research articles.

<table>
<thead>
<tr>
<th>String</th>
<th>Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>String 1</td>
<td>&quot;Crypto&quot; OR &quot;Cryptocurrency&quot; OR &quot;Cryptocurrencies&quot;</td>
</tr>
<tr>
<td>String 2</td>
<td>&quot;Fraud*&quot; OR &quot;Scam*&quot; OR &quot;Crime*&quot;</td>
</tr>
</tbody>
</table>

We inserted a mix of Boolean keywords based on title, abstract, and keyword format into Scopus; TITLE-ABS-KEY("Crypto" OR "Cryptocurrency" OR "Cryptocurrencies") AND ("Fraud*" OR "Scam*" OR "Crime*")) to find the initial sample database for this study. The initial search yielded 1059 documents from the Scopus database.

Therefore, we applied the inclusion and exclusion criteria to our primary search results to screen more relevant papers. We considered our search for the following subject areas: Economics, Econometrics, Finance, Business Management, Accounting, and Social Sciences. We selected journal, book chapters, and review papers in our search process and limited our analysis to the English language and final papers. These inclusion and exclusion criteria helped to improve the quality of the sources by removing 806 irrelevant papers, and the initial sample was reduced to 253 articles for further evaluation. In the next phase, we thoroughly examined the title, abstract, keyword, and conclusion of each paper to include only the most relevant and closely related literature for our research on cryptocurrency-related financial crimes, scams, and frauds. After eliminating 83 documents that were not pertinent to our research theme, we were able to refine our sample for full-text document analysis.

In the final stage, we conducted a full-text screening analysis of the remaining 170 documents to ensure that the studies were aligned with the objectives of our research agenda. We diligently assessed each article on an individual basis and assigned a score of 1 to articles that were within the scope and did fit within the framework of our study; otherwise, we assigned 0. Most of the discarded articles are related to cryptocurrency mining methods and technologies, the crypto biometric process, graph theory in cryptocurrency, cryptocurrency algorithms, cryptocurrency trading, cryptocurrency history, and machine learning use cases in crypto. The final objective is to finalize the set of documents on cryptocurrency-related scams, crimes, or fraud for bibliometric analysis. This evaluation process led to 111 documents that we considered for the final analysis.

Bibliometric analysis is an effective method for exploring and analyzing vast quantities of scientific data. It provides invaluable insight for researchers seeking to comprehend the evolutionary nuances of a specific field, as well as identifying
emerging research areas. The utilization of statistical measurements through bibliometric analysis has the potential to revolutionize the review process for science and scientific activity (Donthu et al., 2021). It offers a systematic, transparent, and reproducible method that could significantly impact how we evaluate science and scientists. It can examine cryptocurrency fraud structures, identify crucial research elements that underlie crypto crimes, highlight the existing gaps in the current research arena, and position researchers for contributions in this relevant discipline. We also performed a content analysis on our dataset to investigate and evaluate important research agendas in cryptocurrency scams. The combination of the quantitative bibliometric method with the qualitative content analysis approach will enhance the credibility and trustworthiness of our research topic.

We used VOSviewer, the Biblioshiny R package, and Microsoft Excel software to analyze our final research sample for bibliographic analysis and content analysis. VOSviewer was used for network mapping analysis, which included bibliographic coupling and cocitation networks, as well as keyword co-occurrence of green bonds in clean energy. Additionally, we utilized the Biblioshiny R package and Microsoft Excel to analyze publication trends, sources, university affiliations, and countries' research contributions to cryptocurrency-based crimes and fraud. Content analysis is performed on the bibliographic coupling of authors and keyword occurrence clusters to identify the subareas of the analysis and insight into the research.

Figure 1 PRISMA Methodology.
3. Research Question 1

3.1. Summary Statistics

Table 2 compiles the summary statistics of the bibliometric analysis of cryptocurrency crimes conducted between 2015 and 2023. This sample of research data from the Scopus database comprises 111 documents, 278 authors, and 80 sources. The 111 documents included in this study included 92 articles, 5 conferences, and 14 review papers. These documents have 334 authors’ keywords and 5219 cited references, with 27 single-author documents and 84 collaborative outputs. This table also shows that the average number of citations per document is 17.32, and the annual scientific production growth is 63.32%. A total of 23.42% of the coauthors are international, and the number of co-authorships per document is 2.69.

<table>
<thead>
<tr>
<th>Description</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timespan</td>
<td>2015:2023</td>
</tr>
<tr>
<td>Sources</td>
<td>80</td>
</tr>
<tr>
<td>Documents</td>
<td>111</td>
</tr>
<tr>
<td>Annual Growth Rate %</td>
<td>63.32</td>
</tr>
<tr>
<td>Document Average Age</td>
<td>2.14</td>
</tr>
<tr>
<td>Average citations per doc</td>
<td>17.32</td>
</tr>
<tr>
<td>References</td>
<td>5219</td>
</tr>
<tr>
<td>Keywords Plus</td>
<td>255</td>
</tr>
<tr>
<td>Author’s Keywords</td>
<td>334</td>
</tr>
<tr>
<td>Authors</td>
<td>278</td>
</tr>
<tr>
<td>Authors of single-authored docs</td>
<td>27</td>
</tr>
<tr>
<td>Single-authored docs</td>
<td>28</td>
</tr>
<tr>
<td>Co-Authors per Doc</td>
<td>2.69</td>
</tr>
<tr>
<td>International co-authorships %</td>
<td>23.42</td>
</tr>
<tr>
<td>Article</td>
<td>92</td>
</tr>
<tr>
<td>conference paper</td>
<td>5</td>
</tr>
<tr>
<td>review</td>
<td>14</td>
</tr>
</tbody>
</table>

3.2. Publication Overtime

Figure 2 shows the publication trend in cryptocurrency scams. An insignificant number of documents were published between 2016 and 2017, and research was only pioneered after 2017. This shows that the research field is new and indicates novelty in the cryptocurrency fraud research area. In 2018, the number of publications increased dramatically due to Bitcoin acceptance by the Chinese and South Korean governments as a possible mode of payment acceptance, the cryptocurrency mining boom, and institutional investor confidence in cryptocurrency. However, the amount of research on cryptocurrency scams moved between 2019 and 2021 due to mixed opinions on cryptocurrency technology, regulatory concerns, liquidation events, and, most importantly, the FOMO (fear of missing out) effect. The years 2022 and 2023 were highlighted for the exponential growth of research articles on cryptocurrency. In the last five years, between 2019 and 2023, the number of publications increased nearly 3-fold.

Figure 2 Publication Over Time.
3.3 The Most Cited Publications

Table 3 lists the top ten most cited journal documents extracted from the Scopus Index database. We found that the Gandal et al. (2018) article "Price manipulation in the Bitcoin ecosystem", published in the Journal of Monetary Economics with 372 citations, is the most influential article, followed by the Al-Rimy et al. (2018) article "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions", published in Computers and Security with 221 citations, which is the second most cited journal. With 77 citations, Conti et al. (2018), "On the economic significance of ransomware campaigns: A Bitcoin transactions perspective," published in Computers and Security, is the 3rd most popular journal in the world of cryptocurrency scams. We noticed that Computers and Security published two highly referenced journal articles and that the top three most influential journals were published in 2018.

Table 3 The Most Cited Publications.

<table>
<thead>
<tr>
<th>Authors</th>
<th>Title</th>
<th>Year</th>
<th>Source Title</th>
<th>Total Citation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kamps J.; Kleinberg B.</td>
<td>To the moon: defining and detecting cryptocurrency pump-and-dumps</td>
<td>2018</td>
<td>Crime Science</td>
<td>76</td>
</tr>
<tr>
<td>Kethineni S.; Cao Y.</td>
<td>The Rise in Popularity of Cryptocurrency and Associated Criminal Activity</td>
<td>2020</td>
<td>International Criminal Justice Review</td>
<td>68</td>
</tr>
<tr>
<td>Kher R.; Terjesen S.; Liu C.</td>
<td>Blockchain, Bitcoin, and ICOs: a review and research agenda</td>
<td>2021</td>
<td>Small Business Economics</td>
<td>56</td>
</tr>
<tr>
<td>O’Leary D.E.</td>
<td>Open Information Enterprise Transactions: Business Intelligence and Wash and Spoof Transactions in Blockchain and Social Commerce</td>
<td>2018</td>
<td>Intelligent Systems in Accounting, Finance and Management</td>
<td>40</td>
</tr>
<tr>
<td>Barone R.; Masciandaro D.</td>
<td>Cryptocurrency or usury? Crime and alternative money laundering techniques</td>
<td>2019</td>
<td>European Journal of Law and Economics</td>
<td>38</td>
</tr>
</tbody>
</table>

3.4 University Affiliation and Affiliation Over Time

3.4.1 University Affiliation

Figure 3 shows the university or institutional affiliation regarding the number of studies published on cryptocurrency scam research. The University of College London in England is the most productive university, publishing 8 papers. The American University of Sharjah in the UAE, Beijing University of Posts and Telecommunications in China, and the University of Southern California each published 6 research papers. Macquarie University in Australia published 5 papers. Two of the top ten research institutions are from England, two are from Australia, and the rest are from the United States, Czech Republic, UAE, China, South Korea, and Saudi Arabia.

3.4.2 University Affiliation Over Time

Figure 4 illustrates the institutional affiliation in cryptocurrency crime research over time. Before 2018, there were no published journals or any contributions from institutions. The University of South Carolina published the first paper in 2018. In 2019, Macquarie University contributed 5 research articles. In 2020, there was a massive spike in cryptocurrency-based
research, and many universities started to publish. Beijing University of Posts and Telecommunications published 6 papers, Brunel University London published 4 papers, Bond University published 4 articles, and Teichmann International Schweiz Ag Consultancy Firm published 2 papers in 2020. The University of South Carolina published 5 papers in 2021, and the University College of London published 7 articles in 2022. In 2023, Narjan University and the American University of Sharjah published 4 papers each.

Figure 3 Article Affiliation.

Figure 4 Article Affiliation Over Time.

3.5. Authors’ Country Collaboration, Country Publication, Country Citation, Countries’ Article Production over Time, and Country Collaboration MAP

3.5.1. Author’s Country Collaboration

Figure 5 shows the collaboration of the top ten corresponding authors based on multiple-country publications (MCPs) and single-country publications (SCPs). The USA ranks first in single-country article collaboration, with 9 published papers, and Indonesia ranks first in multiple countries’ author collaboration, with 3 published papers. Most research articles from the
UK, Australia, Germany, and the Netherlands are SCP contributors. The MCP ratio for Italy is the highest in developed countries at 67%, and articles produced by Indonesia have 100% of the authors’ collaboration with multiple countries.

![Figure 5 Country Collaboration.](image)

### 3.5.2. Country Publications and Citations

Table 4 illustrates the top 10 contributing countries that have published the most articles and gained the most citations in cryptocurrency fraud research. The USA has become the top contributing country in the world, with a total of 10 articles and 567 citations. The UK is second with 9 papers, followed by Australia and Germany, each with 7 papers. Asian countries such as China, the UAE, Indonesia, and Saudi Arabia are among the top-performing countries with 5, 4, 3, and 3 articles, respectively. The Netherlands and Italy are other developed countries on the list, each with 3 papers. In terms of citations, Malaysia holds the second position, with 221 citations and only one paper, and the United Kingdom is in third position, with 187 citations. China is the only Asian country on the top list, followed by Malaysia with citations. The other developed countries that have a position in the citation list are Italy, the Netherlands, Australia, Germany, Norway, and Ireland, with 124, 80, 76, 65, 56, and 47 citations, respectively.

<table>
<thead>
<tr>
<th>Country</th>
<th>No of Publications</th>
<th>Country</th>
<th>No of Citations</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>10</td>
<td>USA</td>
<td>567</td>
</tr>
<tr>
<td>UNITED KINGDOM</td>
<td>9</td>
<td>MALAYSIA</td>
<td>221</td>
</tr>
<tr>
<td>AUSTRALIA</td>
<td>7</td>
<td>UNITED KINGDOM</td>
<td>187</td>
</tr>
<tr>
<td>GERMANY</td>
<td>7</td>
<td>ITALY</td>
<td>124</td>
</tr>
<tr>
<td>CHINA</td>
<td>5</td>
<td>NETHERLANDS</td>
<td>80</td>
</tr>
<tr>
<td>UNITED ARAB EMIRATES</td>
<td>4</td>
<td>CHINA</td>
<td>78</td>
</tr>
<tr>
<td>INDONESIA</td>
<td>3</td>
<td>AUSTRALIA</td>
<td>76</td>
</tr>
<tr>
<td>ITALY</td>
<td>3</td>
<td>GERMANY</td>
<td>65</td>
</tr>
<tr>
<td>NETHERLANDS</td>
<td>3</td>
<td>NORWAY</td>
<td>56</td>
</tr>
<tr>
<td>SAUDI ARABIA</td>
<td>3</td>
<td>IRELAND</td>
<td>47</td>
</tr>
</tbody>
</table>

### 3.5.3. Countries’ article production over time

Figure 6 illustrates the country’s production over time between 2015 and 2023. The graph shows that no countries had any significant research outcomes until 2016. The USA was at the forefront of research in 2016. However, between 2016 and 2018, the number of publications increased slightly for a few countries, such as the Netherlands, Australia, and the UK. However, the USA still dominated its position, with 9 scientific publications. We noticed that in 2019 and 2020, Ukraine saw a steady increase in production, while the USA and Australia continued their position in research. In 2021, cryptocurrency crime research increased in the USA, the UK, and Ukraine. Between 2022 and 2023, the USA, China, and the UK experienced
remarkable growth in publication. Among all countries, the USA showed a steep increase in the number of articles published consistently over the years.

Figure 6 Countries’ Article Production Overtime.

3.5.4. Country Collaboration Map

Figure 7 illustrates the country collaboration map, showing the author’s affiliation with countries involved in cryptocurrency fraud research. In the collaboration map, the thickness of lines is used to show the collaboration frequency among the authors in different countries, and the intensity of the color is used to represent the number of publications in a country. The most robust collaboration was found between the USA and the UK, with 3 papers, followed by the USA and China and then Australia and Canada, each with 2 papers. We observed that the USA, the UK, and Australia are the top three collaborative countries that network with other countries’ researchers, with 14, 7, and 6 collaborations, respectively.

Figure 7 Country Collaboration Map.
3.6. Article Sources and Citation

Table 5 presents the top sources for the articles based on the h-index and g-index. The Journal of Money Laundering and Control is the top-ranked publisher producing cryptocurrency research, with an h-index of 6 and a g-index of 9. It published the most (6) papers, followed by the Journal of Financial Crime, which had the second most (9) papers with an h-index of 3 and a g-index of 6, and Forensic Science International, Digital Investigation, with an h-index of 3 and a g-index of 6. Computers and Security published 4 papers, Computer Fraud and Security published 3 papers, and Risks published 3 papers. The remaining sources in the list each contributed 2 papers. In terms of citations, Computers and Security received a maximum of 333 citations, followed by Crime Science, Journal of Financial Crime, and Journal of Money Laundering and Control with 115, 113, and 113 citations, respectively. The oldest journal in our research sample was published by the Hastings Law Journal in 2016.

<table>
<thead>
<tr>
<th>Sources</th>
<th>h-index</th>
<th>g-index</th>
<th>TC</th>
<th>NP</th>
<th>PY_start</th>
</tr>
</thead>
<tbody>
<tr>
<td>JOURNAL OF MONEY LAUNDERING CONTROL</td>
<td>6</td>
<td>9</td>
<td>113</td>
<td>9</td>
<td>2017</td>
</tr>
<tr>
<td>COMPUTER FRAUD AND SECURITY</td>
<td>3</td>
<td>3</td>
<td>57</td>
<td>3</td>
<td>2018</td>
</tr>
<tr>
<td>COMPUTERS AND SECURITY</td>
<td>3</td>
<td>4</td>
<td>333</td>
<td>4</td>
<td>2018</td>
</tr>
<tr>
<td>FORENSIC SCIENCE INTERNATIONAL: DIGITAL INVESTIGATION</td>
<td>3</td>
<td>5</td>
<td>61</td>
<td>5</td>
<td>2020</td>
</tr>
<tr>
<td>JOURNAL OF FINANCIAL CRIME</td>
<td>3</td>
<td>6</td>
<td>113</td>
<td>6</td>
<td>2018</td>
</tr>
<tr>
<td>CRIME SCIENCE</td>
<td>2</td>
<td>2</td>
<td>115</td>
<td>2</td>
<td>2018</td>
</tr>
<tr>
<td>JOURNAL OF RISK AND FINANCIAL MANAGEMENT</td>
<td>2</td>
<td>2</td>
<td>14</td>
<td>2</td>
<td>2020</td>
</tr>
<tr>
<td>LAWS</td>
<td>2</td>
<td>2</td>
<td>16</td>
<td>2</td>
<td>2021</td>
</tr>
<tr>
<td>RISKS</td>
<td>2</td>
<td>2</td>
<td>8</td>
<td>3</td>
<td>2023</td>
</tr>
<tr>
<td>SMALL BUSINESS ECONOMICS</td>
<td>2</td>
<td>2</td>
<td>86</td>
<td>2</td>
<td>2021</td>
</tr>
</tbody>
</table>

3.7. Author Articles and Citations

Table 6 shows the top authors, their number of publications, total citations, average citations per publication, h-indexes, and their affiliations. Among the authors in the list, both Gleason K. and Kleinberg B. published a maximum of 6 papers on cryptocurrency crimes with an h-index of 3, but Kleinberg B. amassed the highest number of citations, 121. The remaining authors in the list each published 2 papers. Irwin Asm published the oldest paper on the list in 2017. The second most-cited author in the list is Kamps J., with 115 citations, and ranks at the top regarding average citations per paper. One author published papers in 2017, 2 authors published papers in 2018 and 2020, 1 author published papers in 2021, and 4 authors started publication in 2022 on cryptocurrency-related scams.

<table>
<thead>
<tr>
<th>Authors</th>
<th>Affiliations</th>
<th>h-index</th>
<th>TC</th>
<th>NP</th>
<th>AC</th>
<th>PY Start</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gleason K.</td>
<td>Department of Finance, School of Business Administration, American University of Sharjah, Sharjah, United Arab Emirates</td>
<td>3</td>
<td>37</td>
<td>3</td>
<td>12.33</td>
<td>2021</td>
</tr>
<tr>
<td>Kleinberg B.</td>
<td>Department of Methodology and Statistics, Tilburg University, Tilburg, The Netherlands</td>
<td>3</td>
<td>121</td>
<td>3</td>
<td>40.33</td>
<td>2018</td>
</tr>
<tr>
<td>Akartuna Ea</td>
<td>Department of Security and Crime Science, University College London, England</td>
<td>2</td>
<td>42</td>
<td>2</td>
<td>21.00</td>
<td>2022</td>
</tr>
<tr>
<td>Davies T.</td>
<td>Department of Security and Crime Science, University College London, England</td>
<td>2</td>
<td>45</td>
<td>2</td>
<td>22.50</td>
<td>2022</td>
</tr>
<tr>
<td>Dupuis D.</td>
<td>Department of Finance, School of Business Administration, American University of Sharjah, Sharjah, United Arab Emirates</td>
<td>2</td>
<td>34</td>
<td>2</td>
<td>17.00</td>
<td>2021</td>
</tr>
<tr>
<td>Falkner M.C.</td>
<td>Teichmann International (Schweiz) AG, St. Gallen, Switzerland</td>
<td>2</td>
<td>37</td>
<td>2</td>
<td>18.50</td>
<td>2020</td>
</tr>
<tr>
<td>Irwin A.S.M.</td>
<td>Macquarie University, Sydney, Australia</td>
<td>2</td>
<td>51</td>
<td>2</td>
<td>25.50</td>
<td>2017</td>
</tr>
<tr>
<td>Johnson S.D.</td>
<td>Department of Security and Crime Science, University College London, England</td>
<td>2</td>
<td>42</td>
<td>2</td>
<td>21.00</td>
<td>2022</td>
</tr>
<tr>
<td>Kamps J.</td>
<td>Department of Computer Science, VU University Amsterdam, Amsterdam, The Netherlands</td>
<td>2</td>
<td>115</td>
<td>2</td>
<td>57.50</td>
<td>2018</td>
</tr>
<tr>
<td>Mackenzie S.</td>
<td>Faculty of Humanities and Social Sciences Victoria University of Wellington, New Zealand</td>
<td>2</td>
<td>34</td>
<td>2</td>
<td>17.00</td>
<td>2022</td>
</tr>
</tbody>
</table>

3.8. Keyword Analysis

3.8.1. Author keywords

https://www.malque.pub/ojs/index.php/mr
Figure 8 shows the frequency of keywords in the literature related to cryptocurrency and its association with financial crimes. 'Cryptocurrency' is the main keyword with 68 occurrences, constituting almost 35% of the total frequency. The frequency of other keywords has been analyzed to examine their relationship with research in the cryptocurrency field. Bitcoin is another primary keyword, representing 16% of the total frequency. Money laundering and blockchain each represent 10% of the total frequency of their use, with 20 and 19, respectively, whereas other keywords such as fraud, financial crimes, crimes, regulation, fintech, and cybercrime have less than 10% of the total frequency.

3.8.2. Keyword trends

VOSviewer has been used to determine frequently used keywords and to identify research trends. Figure 9 highlights the keyword trends in research in the 2018–2023 era. In the early era (2018–2020) of cryptocurrency-related research, keywords such as ransomware, bitcoin, and cybercrime dominated the relevant literature. Among these three keywords, bitcoin was the most dominant, with 32 mentions. The topic of "cryptocurrency", with 68 mentions, has dominated the research focus from 2020–2023. Other keywords, such as money laundering (19 times), blockchain (20 times), and fraud (17 times), have also been focal points. The frequencies of financial crime, regulation, crime, and fintech are ten times less. A significant part of the studied literature reveals that cryptocurrency-related illegal activities have been committed mainly through fintech-based techniques in recent years. For instance, criminals commit money laundering through Bitcoin cards preloaded with virtual currency (Sanz-Bas et al., 2021). Fraudsters employ phishing tricks via fake emails to entice victims to share sensitive information. They lure investors to deposit funds in fake wallets or exchanges (Nikkel, 2020).

3.9. Cocitation analysis

In bibliometric studies, cocitation assessment is one critical aspect of understanding how related research works are intertwined. A cocitation occurs when two studies are cited together in a third study. The cocitation analysis of authors provides insights into how those studies contributed to the evolution of concepts within a particular field. It is a popular method for comprehending the field’s intellectual framework. For this study, a cocitation analysis of authors was conducted using VOSviewer software. The analysis included 49 items (authors or works) that met the threshold set for the analysis, which in this case was a minimum of 10 citations per author or work. The chosen studies formed five clusters corresponding to various topics or subfields within the larger research field under analysis. These studies have 817 ties between them, which suggests a sizable number of cocitation relationships. The overall degree of cocitation among the components is shown by the total link strength of 7827.

Figure 10 presents a network visualization where authors are represented as circular nodes and cocitations as lines connecting these nodes. The five observable clusters of studies are yellow, green, red, blue, and purple. Each cluster contains a list of authors frequently cocited together, suggesting that they have contributed to the same subfield or topic. For example, Cluster 1 has 16 items, Cluster 2 has 13 items, Cluster 3 has 11 items, and so on. The authors within each cluster share a thematic or methodological connection in their works.
The scatteredness or expanse of each cluster denotes the degree of cocitation of the authors. In contrast, the connecting lines' density represents the cocitation relationships' robustness. Authors belonging to the same cluster are more likely to be referenced together in a publication, and the size of an author's circle indicates how frequently they are cited. The distance between nodes indicates the relatedness of the authors' work. Closer nodes suggest a more substantial relationship or more significant cocitation. The delineated clusters exhibit distinct author groupings in the cocitation network analysis visualized by VOSviewer. The red cluster comprises Nakamoto S., Gottschalk P., Christin N., and Holt T.J.; the yellow
cluster is characterized by the inclusion of Smith L.M., Kamps J., and Kleinberg B.; the green cluster encompasses Moore T., Chen W., Gandal N., and Luo X.; the blue cluster consists of McCoy D. and Bonneau J.; and the purple cluster is represented by Corbet S. and Larkin C., indicating potentially thematic or disciplinary connections among the authors within each cluster. In the red cluster, the work of Nakamoto; in the yellow cluster, the work of Smith; in the green cluster, the work of Moore; in the blue cluster, the work of McCoy; and finally, in the purple cluster, the work of Corbet is closely linked to the other clusters as well as fellow cluster companions.

3.10. Thematic Study

A thematic study uses keyword co-occurrence analysis to decipher the development of research themes in a particular field, and these themes are divided into four quadrants: motor, niche, emerging or declining, and basic (Nasir et al., 2021; Kashi & Shah, 2023). These four topologies demonstrate research concentration in a particular field according to their density and centrality (Abhilash et al., 2022). Density signifies the importance of a theme, while centrality highlights the volume of work done on a specific theme and its capability to develop (Agbo et al., 2021). This analysis aims to identify the potential research developments in the thematic areas of cryptocurrency in Figure 11.

![Thematic Study](https://www.malque.pub/ojs/index.php/mr)

**Figure 11** Thematic Study.

In the first quadrant, the motor themes, with their high density and centrality, constitute the topics that are adequately studied, well developed, and central to the field. These themes in the cryptocurrency field include keywords such as money laundering, blockchain, regulation, and crime. Blockchain technology is the foundation of developing and functioning digital assets such as cryptocurrency. Therefore, it is central to the discussion of cryptocurrency. Furthermore, the cryptocurrency industry is not adequately regulated, making it a safer vehicle for conducting crimes such as money laundering, another theme that is also well developed and highly relevant in crypto research.

Niche themes in the second quadrant have high density but low centrality, highlighting the essential themes that are less studied in the field. According to the findings in the graph, topics such as digital currency, cybersecurity, investigation, and digital forensics have a high degree of development. However, they need further connections to cryptocurrency research. Tools such as cybersecurity and digital forensics can be effective in mitigating cryptographic crimes. These topics are significant in cryptocurrency, and future research will benefit the field.

The themes in the third quadrant have low centrality and low impact. These topics have more scope for future research or might decline from the literature. Themes such as cybercrime, anti-money laundering, and phishing are topics closely related to cryptocurrency crimes that researchers are focusing on or are no longer interested in examining.

The fourth quadrant contains basic themes with high centrality but low density. These topics are fundamental to the literature on cryptocurrency and crucial for developing the field. Keywords such as cryptocurrency, financial crime, and bitcoin are themes that contribute to the advancement of cryptocurrency research.

Overall, the thematic map suggests that cryptocurrency research primarily covers themes related to cryptocurrency crimes. These topics include money laundering, cybercrime, phishing, cybersecurity, digital forensics, anti-money laundering, and financial crime. While some of these topics are well developed and relevant to crypto research, researchers can explore them further. Money laundering, one of the top crimes in crypto, is already a well-developed and highly relevant theme. However, cybersecurity and digital forensics are well-developed themes. However, they need to be more relevant to crypto
research but may be able to be developed in future studies. Cybersecurity and digital forensics can protect crypto users from online miscreants (Dolejška et al., 2023; Nikkel, 2020).

Anti-money laundering can be a valuable tool, as lawmakers aim to minimize financial crimes involving money laundering. Given the abundance of crimes in crypto, researchers should underscore these topics in their studies. Apart from crime-related themes, other themes that are relevant to the field include Bitcoin, digital currency, and blockchain. Bitcoin is the first cryptocurrency and, therefore, is a well-discussed topic in cryptocurrency. Blockchain technology is the foundation of cryptocurrency (Castonguay & Stein Smith, 2020); therefore, it is a central topic in crypto research. The topic of digital currency, while having a certain degree of development, is not highly relevant to cryptocurrency. Cryptocurrency is a form of digital currency; therefore, this topic has further scope for development in future studies.

3.11. Factorial Analysis

Factorial analysis is a statistical analysis used to identify the intellectual structure of research papers in a field by showing the relative distribution and distance of keywords or research topics (Abhilash et al., 2022). Usually, two clusters (red and blue) categorize the main themes of research papers in a field. The words closest to the map are associated with and well studied in the literature, and the words on the edges have been less studied in cryptocurrency research (Figure 12).

In the red cluster, words such as the Liechtenstein Blockchain Act, terrorist financing, regulation, malware, cybersecurity, scams, and decentralized finance are on the edges. Notably, these topics could be more interconnected in crypto research. In contrast, words such as money laundering, financial crime, fraud, and digital forensics are closely associated. These terms primarily relate to cryptocurrency crimes, forming a cohesive network of related themes. The keywords in the blue cluster include fintech, virtual currency, darknet, USA, and financial regulation. Most of these keywords are on the edges of the cluster. These topics have potential for future research to develop the domain of cryptocurrency research.

4. Content Analysis

4.1. Keyword Co-Occurrence

Keyword co-occurrence analysis is an efficient research tool for identifying related literature and trends. The co-occurrence network of keywords is highlighted in Figures 13 and 14. Of the 334 keywords, only 15 met the minimum threshold criteria. These 15 keywords were divided into 4 clusters. Each of the clusters has been titled by the most frequently mentioned keyword of that cluster. “Cluster (Red): Blockchain & Money Laundering” contains five keywords: anti-money laundering, blockchain, financial crime, fintech, and money laundering. “Cluster (Green): Bitcoin” involves four keywords: bitcoin, cybercrime, malware, and ransomware. “Cluster (Blue): Regulation” includes digital assets, virtual currency, and regulation keywords. Finally, “Cluster (Yellow): Cryptocurrency & Frauds” contains crime, cryptocurrency, and fraud keywords. Although keywords are separated into different clusters, the contents of each cluster are connected to the contents of other clusters. For instance, the cluster ‘yellow’ cryptocurrency has been discussed in papers related to blockchain and money laundering (cluster ‘red’) and bitcoin (cluster ‘green’).
4.1.1. Cluster (Red): Blockchain & Money Laundering

Blockchain technology acts as a public ledger containing details of past transactions. This technology provides security and privacy and eliminates the need for intermediaries. Blockchain provides the basis for many cryptocurrencies. Prendi et al. (2023) stated that the main features of cryptocurrency, i.e., confidentiality, speed, and global reach, that attract legitimate users also attract criminals. Castonguay & Stein Smith (2020) mentioned that cryptocurrencies are vulnerable to manipulation and malfeasance due to their characteristics. Money laundering via cryptocurrency occurs in three phases: 'placement,' 'layering,' and 'integration.' Criminals misuse the advantages of confidentiality, security, and privacy to launder money through virtual exchanges, mixers, and online video games such as 'Fortnite' (Sanz-Bas et al., 2021). Gaviyau & Sibindi (2023) discussed the current development in customer due diligence (CDD) in this fintech era. They investigated how technological innovations shape and guide customer due diligence (CDD) in the anti-money laundering (AML) discipline. Sun et al. (2022) and Sabuj et al. (2024) proposed a KYC (know your customer) compliant identity scheme. The scheme allows only the users to know their identity and wallet accounts, thus providing privacy and confidentiality, while supervisors can trace the identities of suspicious accounts. Technological solutions that could be included in anti-money laundering spheres are still being developed. Although most current legislation falls short in effectively handling money laundering through cryptocurrency, The Tokens and TT Service Provider Act (abbreviated as TVTG)” proved efficient, as the Liechtenstein Government Act introduced a comprehensive blockchain act. Unlike other legislations in the EU or the USA that focus on cryptocurrencies only, TVTG rules go a step further in encompassing all potential uses of blockchain (Teichmann & Falkner, 2020).

4.1.2. Cluster (Green): Bitcoin

Bitcoin, a cryptocurrency founded on blockchain, is often received as a payment in ransomware and malware attacks by criminals. Ransomware is malware that utilizes cryptography to control users’ files and resources and demand payment in return for unlocking data. A detailed taxonomy of ransomware has been developed based on target, platform, and severity (Al-rimy et al., 2018). Keeping backup data, employing security tools, ensuring email security, updating software, and operating systems, and accessing and authorizing controls are some mitigating techniques for such attacks. However, reducing the number of such malware attacks relies on high user awareness (Nadir & Bakhshi, 2018). Proper ransomware
identification is the first step in ascribing cybercrime features to an incident. In general, malware attacks can be categorized into web browser-based crypto mining binary crypto mining. Such categorization has been developed based on malware code and behavioral analysis to investigate sophisticated crypto-mining attacks (Zimba et al., 2018). Applying a target-centric intelligence approach in analyzing ransomware attacks can provide intelligence units with an appropriate framework to deconstruct the financial aspect and model the network behavior of illegal Bitcoin transactions (Turner et al., 2019). Another proposed framework starts by identifying Bitcoin addresses related to the ransomware, collecting data from the blockchain, and then categorizing the payments as ransoms (Conti et al., 2018). Current regulations must be more robust to cover the scope of ransomware and other cybercrime attacks. For any regulatory framework to be practical, it is essential to guarantee consistency, clarity, and cost-effective implementation (Irwin & Dawson, 2019).

4.1.3. Cluster (Blue): Regulation

While discussing digital assets and virtual currency, most of the research articles have narrowed their focus on cryptocurrencies such as Monero, Bitcoin, and Ethereum since they are currently popular forms of virtual currency. Kethineni & Cao (2019) identified the characteristics of virtual currency supporting financial crimes and the effects of politics in developing regulations for virtual currencies. Continuous changes in the payment system and the inclusion of virtual currencies such as Apple Pay and Bitcoin have added to these difficulties. Public law needs to be more efficient in regulating the operational side of the payment system (Burge, 2016). International cooperation is essential for combating virtual currency-related financial crimes. However, more uniformity is needed in different legislation on virtual currency, digital assets, and cryptocurrencies across different countries, which hinders the development of an international regulatory framework. The risk-based approach of the FATF (Financial Action Task Force) can prove to be an efficient method for coordinating the efforts of regulatory bodies in handling such financial crimes (Kreminsky et al., 2021). The law of Ukraine’s "On Virtual Assets" does not include cryptocurrency properly within its scope. Due to such limitations, the Criminal Code cannot prosecute criminals for illegal possession or provide shelter to legitimate users (Kozii, 2023). Dhali et al. (2023) examined the virtual currency-related regulations of four jurisdictions, i.e., the USA, Canada, China, and the EU, to evaluate the sustainability of these regulations. Sanz-Bas et al. (2021) analyzed the current regulations adopted by the European Union and the Spanish Government. The EU’s ‘Fifth Directive' was published in 2018, and FATF’s "Guide on Virtual Assets and Virtual Asset Service Providers" guides the Spanish financial system in regulating virtual currencies. One major problem indicated by these research articles is the difference in political and legal stances across countries regarding the acceptance of virtual currency.

4.1.4. Cluster (Yellow): Cryptocurrency & Frauds

While research streams discussed in previous clusters have highlighted cryptocurrencies and their link to money laundering, ransomware, malware, and cybercrime, the 'Yellow' cluster focuses on research trends in cryptocurrency, fraud, and crimes. Cryptocurrencies depend on networks such as the Internet, which is an imperfect network with incomplete information, uncertainty, and delays. Such drawbacks create an opportunity for fraudsters. One of the common frauds occurring in the realm of cryptocurrency is 'Double-Spending Fraud' (Li & Wang, 2022). Nonfungible Tokens (NFTs), a new development in cryptocurrency, claim to deter fraud by providing authentic and verifiable proof of ownership for digital assets. The potential for unauthorized copying, modification, and deletion of digital assets linked to such tokens would stand in the way (Mackenzie & Bērziņa, 2021). Cryptocurrencies such as Monero and Zcash provide a higher level of confidentiality and reveal very little information about the users. As a result, they are complexly regulated and preferred by fraudsters (Kfir, 2020). Some research articles have examined the shared characteristics of these crypto scammers and the similarities of their techniques. Some common characteristics are using incorrect spelling, creating a sense of urgency and fear of missing out, requesting victims incessantly to show screenshots of payments, etc. (Chergarova et al., 2022). Fraudulent activities occur through social media, such as Facebook, Telegram, Signal, Twitter, and Instagram. Twitter is more careful in handling spam content than other platforms. The volatility of the market, absence of proper regulations, and risk of online behavior have contributed to the success of these fraud schemes (Lacey et al., 2020).

4.2 Bibliographic Coupling

The bibliographic coupling of themes is a variation of the standard bibliographic coupling concept, which focuses more on thematic similarities between documents. This approach considers the shared references between two documents and how these references are used within any topic context, as shown in Figure 15. Bibliographic coupling of documents was conducted using the VOSviewer tool, creating clusters based on shared themes identified through similarities among the studies. Only articles that were cited at least 12 times were considered to be the most representative studies. From an initial pool of 111 articles, the 18 most cited articles were chosen for detailed cluster analysis. Consequently, these 18 articles were divided into four distinct clusters, each categorized according to a shared thematic focus, which emerged from the selection and citation patterns observed in the articles.
Cluster one covers the articles discussing the usage of cryptocurrency in illicit activities, the regulatory challenges it imposes, and the legal implications. Broadhead (2018) highlights the dynamic nature of cybercrime, noting the significant impact and growth of malware, especially ransomware, and the evolving use of darknets and cryptocurrencies in criminal activities. The study also emphasized the challenges in measuring cybercrime costs and the diverse nature of cybercrime agents, including organized crime groups, state-affiliated actors, and individual hackers. Dupuis & Gleason (2021) identified various methods, such as tumblers, over-the-counter (OTC) markets, privacy coins, decentralized exchanges, direct retail purchases, and mining fronts, as the means for laundering money. The paper emphasized that while cryptocurrencies offer some anonymity, they are not entirely untraceable, and legal and regulatory frameworks continue to evolve in response to these challenges. Kamps & Kleinberg (2018) investigated the phenomenon of pump-and-dump schemes in the cryptocurrency market. This research introduced methods for identifying potential pump-and-dump activities using anomaly detection techniques, focusing on price and volume anomalies. The study revealed that these schemes are prevalent and often centered on cryptocurrencies with low market capitalization. The findings stress the importance of regulatory measures to address these fraudulent activities in the cryptocurrency market. Nadir & Bakhshi (2018) emphasized the increasing sophistication of ransomware, the use of cryptocurrencies for payments, and the need for robust cybersecurity measures. The paper also provided preventive recommendations and discussed the financial and long-term implications of ransom payments. Sanz-Bas et al. (2021) discussed the risks of using cryptocurrencies in illegal activities such as money laundering and fraud. Various methodologies used in these illicit practices, such as mining, exchanges, and online video games and mixers, have been explored. This paper focused on balancing the benefits of cryptocurrencies with the need for effective regulation to mitigate associated risks.

Cluster Two sheds light on the crypto ecosystem and the dual nature of crypto usage. Trozze et al. (2022) discussed cryptocurrencies’ dual role in facilitating and combating financial crime. There is a need to balance the advantages and risks of cryptocurrencies in the context of financial crime. Phillips & Wilder (2020) described the methods and strategies used in cryptocurrency scams and provided insights into detecting and preventing such scams. Gandal et al. (2018) addressed the vulnerability of the Bitcoin market to price manipulation. These manipulations have profound effects on the market’s stability and credibility. Hornuf et al. (2022) discussed initial coin offerings (ICOs) and their potential as alternatives to traditional financing methods. This paper emphasized the need for clear regulatory frameworks to ensure investor protection and guide the growth of ICOs.

Cluster three focused on the societal impact of technological innovation. It also pinned down the need for interdisciplinary research in criminology, economics, and computer science to understand and address the challenges posed by technology. Mackenzie (2022) focused on the gray economy and cryptocurrency scams. This paper discussed the gradual shift toward a ‘metaverse’ way of living, blending online and offline experiences. Kher et al. (2021) investigated various
blockchain-related fields, such as computer science, economics, entrepreneurship, and law and governance. This paper outlined how these disciplines interact with and are impacted by blockchain technology. Almaqableh et al. (2023) demonstrated the intersection of criminal activities and cryptocurrency markets, highlighting the role of cryptocurrencies in facilitating illegal drug transactions.

Figure 15 Bibliographic Coupling.

Cluster four revealed the tracking difficulties of cryptocurrency footprints in illegal activities. Irwin & Dawson (2019) have discussed the difficulties in tracing cryptocurrencies used in cybercrimes, particularly ransomware attacks, and the ineffectiveness of current regulations. This paper emphasized the need for consistent, clear, and cost-effective regulatory frameworks to address these challenges, enhance legal definitions, and aid cybercrime investigations. Kethineni & Cao (2020) focused on the difficulties that authorities face in tracking and regulating cryptocurrencies due to their anonymity, cross-border nature, and inconsistent global regulations. On the other hand, Reynolds & Irwin (2017) portrayed the level of anonymity in Bitcoin transactions and the challenges in tracing them back to individuals. All the papers in this cluster recommended the need for enhanced regulation.

Finally, all the papers in these four clusters addressed one common theme: the need for an enhanced regulatory and legal framework for mitigating the risk of cryptocurrency-related crimes and money laundering. This theme underlines the challenge of overseeing a rapidly evolving digital financial landscape, where traditional regulatory approaches often need to be revised. The papers collectively emphasize that the anonymous and decentralized nature of cryptocurrencies makes them appealing for illicit activities, necessitating innovative legal strategies. This recognition points toward an interdisciplinary approach, combining insights from technology, law, finance, and criminology to develop effective measures for crime prevention and regulatory compliance in the cryptocurrency domain.

## 5. Research question 2

### 5.1. Top 10 Cryptocrimes

Cryptocurrency offers a vehicle for anonymous transactions (Teichmann & Falker, 2021). Therefore, law enforcement needs help tracing these transactions back to the owner (Teichmann & Falker, 2021). This feature makes cryptocurrency an attractive method for illicit activity, as shown in Figure 16. The top 10 cryptocurrency crimes found in keyword analysis are given below.

1. **ICO Frauds**: An initial offering is raising capital by selling cryptocurrency, usually by start-ups involved in the digital currency market. ICO frauds encompass various forms. The firm issuing the ICO disappears after collecting money or guarantees an unrealistic return on investment to attract investment and eventually fails to do so (Hornuf et al., 2021). Conversely, ICO issuing firms and their investors can be victims of fraud through phishing, hacking, or malware by online miscreants (Hornuf et al., 2021).
2. Money laundering: Money laundering is a process of legalization of the money earned through illegal transactions. The process involves three steps—placement, layering, and integration (Sanz-Bas et al., 2021). During placement, money launderers purchase cryptocurrency through exchanges, P2P exchanges, or crypto ATMs, and during layering, launderers use unregulated exchanges to trade coins into different digital currencies or use mixers, which allows them to use anonymizing browsers to distort their location (Teichmann & Falker, 2021).


4. Ponzi (pyramid) Schemes: The fraudulent issuers of cryptocurrency circulate false information, make extensive marketing efforts, and offer tempting returns to lure investors into buying, selling, or converting coins and then disappear with the money (Dupuis & Gleasonb, 2021).

5. Pumps and Dumps: The fraudsters circulate misinformation to increase the price of low-valued coins and sell those coins to make profits, leaving investors who bought those coins at a high price with a large number of losses (Hornuf et al., 2021; Trozze et al., 2022). ICO issuing firms are sometimes involved in this type of fraud.

6. Exchange scams: Cryptocurrency exchanges engage in scams by closing the platform after investors buy coins through that exchange (Trozze et al., 2022). FTX was one such exchange that defrauded its investors by misusing funds and moving funds across various entities owned by Sam Bankman-Fried, the owner of FTX. While FTX did not close and disappear with the funds, it misused the funds of its investors, which led to its bankruptcy.

7. Ransomware: Ransomware is a kind of malware designed to attack an individual or organization’s system or computer to take control of that system and deny access to the owner. Hackers threaten to disclose private information or destroy valuable data until victims fulfill ransom demands, usually in digital currency (McCord et al., 2022, and Dupuis & Gleasonb, 2021).

8. Darknet market: Cryptocurrency has become a popular payment method in the darknet market for illegal services such as dealing with illegal drugs and substances, human trafficking, illicit trafficking of protected goods, and counterfeit documents (McCord et al., 2022).

9. Phishing: Scammers create fake websites, links, emails, or social media accounts that closely resemble the official version and, therefore, are difficult to differentiate. The fraudsters use various methods to distribute these false gateways. They use malware, social media marketing, and search engines to replace the original gateways (Dupuis & Gleasonb, 2021). Phishing is common during ICOs. In 2017, when CoinDash started its public ICO phase, attackers changed official wallet addresses and collected 43,000 ETH in seven minutes until CoinDash shut down its website (Dupuis & Gleasonb, 2021).

10. Corruption: Cryptocurrency involves corruption-related fund transfers (such as bribery). Both parties involved in such transactions have a wallet, and they can avoid detection by ensuring that their e-wallets are inaccessible to others (Teichmann & Falker, 2021). Later, they can convert this cryptocurrency into cash through money laundering. Scammers, fraudsters, and unethical individuals commit various crimes in digital currency (Sabuj et al., 2019). According to Trozze et al., 2022, academic research and gray literature have identified 47 unique types of cryptocurrency fraud. Examples of such crimes may include market manipulation, scam wallets, mining scams, identity theft, wire fraud, wash trading, and romance scams (Trozze et al., 2022). The top 10 crimes discussed above are the most widely discussed and known. However, crimes such as Ponzi schemes, ICO fraud, phishing, and pumps and dumps occur more frequently than others (Trozze et al., 2022; Ahammed & Saha, 2018; Hornuf et al., 2021).

5.2 Reasons for Cryptocurrency Fraud

Cryptocurrency has been used to finance various crimes, including money laundering, fraud, facilitating illicit trade, and terrorism. Cryptocurrency has been used for trading illicit goods since its inception in 2008 (Teichmann & Falker, 2021). The earliest use of cryptocurrency, such as Bitcoin, was popularized on dark web platforms such as the Silk Road, but over the years, it has crept into various other criminal activities. Cryptocurrency is pseudoanonymous, accessible across locations that might otherwise be under sanction, and the ease of converting to other fiat currencies, and having no institutional middleman in transactions make crypto a lucrative choice for criminals (Kethineni & Cao, 2020). Cryptocurrency, being a relatively new technology, meant that laws and regulations needed to be entirely up to speed on it, and all these features and conditions meant that cryptocurrencies were increasingly becoming a tool for illegal activities. There is also the underlying philosophy of cryptocurrency, which seeks less regulation and intervention from the central authority and more privacy for the individual traders that could attract the people who seek those attributes because of ill intentions. The recurring factors behind cryptocurrency crimes that were researched are discussed below:

1. Decentralization: Decentralization is one of the cornerstones of cryptocurrency, and while the allure of less regulation invites investors who value privacy and freedom to invest, it could also attract people to evade the financial institutional framework to avoid running into the authorities. Decentralization means that there are no
measures to vet the type of investors operating in the crypto domain, making it easier to commit crimes with cryptocurrency.

2. Access: Another cornerstone of cryptocurrency is that since it is fully digital, any individual can have access at any time from any part of the world. Once again, while this is a great feature, it also means that places under sanction can access cryptocurrency. Additionally, this digitization makes it easy to move money anywhere in the world, making it an excellent tool for laundering money (Van Wegberg et al., 2018), which is one of the most committed crimes using cryptocurrency.

3. Anonymity: The privacy features of cryptocurrency make it possible to participate in trading without publicizing information or interacting directly with the other party, which could influence criminal motivation. The rational choice theory of crime, which is discussed later in this section, describes how anonymity can help a person rationalize crimes.

4. Low barrier to entry: Mining cryptocurrency is easier to follow and kickstart a crypto project compared to a traditional stock, which also means that it is easier to commit initial coin offering (ICO) scams or Rug pull (Kethineni & Cao, 2020) scams where a cryptocurrency project is started with the end goal of scamming and is closed as soon as its goals are met.

5. Ease of Conversion: Another feature of cryptocurrency that works with the access factor for allowing crimes is the ease of converting cryptocurrency to a fiat currency (Van Wegberg et al., 2018). This makes it possible to circumvent geological boundaries, but criminals can also convert cryptocurrency into their preferred currency if cryptocurrency exchanges allow it. This is why cryptocurrency is a dominant currency in illicit trading and money laundering.

6. Speculative Expectation: Cryptocurrency is very volatile as a financial asset, and the large swings in cryptocurrency prices have made it a target of speculative traders and pump-and-dump schemers. Existing research suggests that Cryptocurrency traders are high-risk takers with a significant fear of missing out (FOMO) factor in their judgment. They are much more likely to be younger and more influenced by social media (Sudzina et al., 2023).

7. Investor overconfidence: As mentioned above, many cryptocurrency traders are young and speculative. Studies have shown that cryptocurrency traders are overconfident in agreeableness and extraversion scales and have less self-control (Johnson et al., 2023). Being less versatile in financial acumen but confident about themselves could make them vulnerable to cryptocurrency scams. The technology behind cryptocurrencies is highly mathematical and complicated, making this situation even worse.

8. Lack of Regulation: As a new and complicated technology, cryptocurrencies have different regulatory structures around them, and decentralization makes it difficult to do so as well. The lack of regulation makes it easier for
investors to rationalize committing crimes because they believe they can get away with it (Kethineni & Cao, 2020).

While many factors behind the crimes are related to intrinsic features of the cryptocurrency itself, these also influence the type of investors it draws in. That is why a discussion about whether the type of crowd that cryptocurrency attracts is more susceptible to committing these crimes within the criminology theoretical framework is worthwhile because a proper understanding of what type of people are cryptocurrency investors and why they commit crimes could help revise the regulations and protect the investors.

Some theories that could be used to explain cryptocurrency crimes are discussed below. The theories mainly consider investors willing to commit these crimes, not unsuspecting victims.

5.3. Theories Behind Cryptocurrency Frauds

Some theories that could be used to explain cryptocurrency crimes are discussed below. The theories mainly consider investors willing to commit these crimes, not unsuspecting victims.

5.3.1. Rational Choice Theory

The rational choice theory in criminology dictates that if a crime is profitable and has low risks, an individual could rationalize doing it. This theory is one of the older theories, as it originated in the 18th century through the works of Cesare Beccaria but is still applicable to modern-day crimes. Cybercrimes require no physical contact or confrontation with the involved parties, and an overall lack or lag of regulations around crypto trading has made it lucrative for individuals with criminal intent. As long as the crime (fraud or Ponzi scheme, money laundering services) is profitable, it makes more rational sense to use cryptocurrency if the chance of being caught is lower since cryptocurrencies have robust anonymity features (Janze, 2017). Rational choice, in this case, relies on the perception of the investor, not grounded in objectivity. A cryptocurrency investor with high-risk tolerance and overconfidence is more likely to rationalize engaging in criminal activities with cryptocurrency to maximize his gains.

5.3.2. Convenience Theory

The convenience theory of white-collar crimes put forward by Gottschalk explains that convenience in three dimensions works to enable white-collar crime. Nolasco Braaten and Vaughn (2021) proposed that it also works for cryptocurrency-related crimes. The first is the economic dimension, which is the desire to profit financially from committing the crime (AIS, 2018). Second, the organizational dimension, where criminals have strategic positions in the organization or the hierarchy, gives them more access to resources and more control to commit these crimes. For example, pump and dump scams are common in cryptocurrency trading, where small groups of people who own significant amounts of a coin will use their influence to artificially inflate the price (pump) and sell their share when it is high (dump), so the naïve crypto traders who follow them and buy at high prices will see the price plummet (Mackenzie, 2022). This scheme could not have been performed without access to a large enough share of the coin and influence to move the naïve crypto traders. Additionally, scammers can rig the voting majority (51%) to validate trades if they extend enough control over the launching of a coin, which leads to ICOs and rug pulls. Finally, in the behavioral dimension, criminals can easily justify their actions and rationalize crimes so that they are not guilty about committing them. Cryptocurrency crimes are almost entirely cybercrimes. After anonymity and decentralization, there is no need to engage with victims directly, making these white-collar crimes much easier to address. The convenience theory of crime provides a good framework for understanding crypto-crimes. The decentralized aspect of cryptocurrency makes it much easier for fraudsters to navigate cryptos and get away relatively quickly, and it is profitable to commit crimes.

5.3.3. Social Learning Theory

It is not only that specific cryptocurrencies are used for criminal activities or that certain coins are offered with the intention of fraud (Hornuf et al., 2022) but also that cryptocurrency is used for crimes. The dramatic collapse of the FTX, the cryptocurrency exchange, due to fraudulent activities, and investors nearly collapsing Binance, another crypto exchange, by withdrawing almost $1 billion shows how fickle the cryptospace is and the general lack of faith even down to the trading platform itself. The egalitarian view and desire for privacy and freedom from regulations gave birth to the cashless transaction system of cryptocurrency, but this also attracts crowds seeking to move away from traditional financial institutions and instruments. According to social learning theory, individuals can engage in crime or cybercrime by witnessing the behavior or actions of others. The activities of the crypto trader communities give the impression that market abuse and losing investments in a flash are normalized, and the responsibility falls to the individual to look out for themselves in a trade (Mackenzie, 2022). It is easy for newcomers who could be followers of similar individual responsibility and profit by any means mindset to mimic the behaviors of others and participate in scams and other crimes, whether knowingly or unknowingly. The previous theories presented relied on some distinguishable features of cryptocurrency (anonymity,
virtuality, decentralization, etc.). However, this theory relies more on what cryptocurrency offers beyond monetary means and the culture it promotes. The rise in interest in cryptocurrencies and increased crime gives credence to this theory that many crypto traders follow what they have seen as more prominent and influential players do in the market.

5.3.4. Space Transition Theory

Space transition theory is a more direct interpretation of social learning theory for crimes with cryptocurrency. Space transition theory suggests that people with a repressed or overt tendency to commit crimes in real life are also likely to commit crimes in virtual space due to the anonymity and likelihood of forming bonds with similar tendencies (Jaishankar, 2007). This makes intuitive sense since many people seeking anonymity and needing more governance in financial transactions could be barred from doing so in traditional financial institutions. There could be strong self-selection bias where cryptocurrency is used for illicit financing and crimes because it is used by unsavory individuals who have already committed those crimes in real-world space. It has already been discussed how certain features of cryptocurrency could be useful for committing crimes such as money laundering and scams, so it is unsurprising that real-work money launderers and scammers would start to show in the virtual space to use cryptocurrency for such activities.

6. Research question 3

6.1. Future research agenda, challenges, and proposed research questions

To lessen the impact of ransomware attacks, Nadir & Bakhshi (2018) outlined their future research agenda, which includes investigating the changing landscape of Internet-connected devices, including the IoT, and improving user awareness and response to ransomware threats. To increase the blockchain-based anonymous reporting scheme’s applicability and impact on fostering accountability and transparency, Wang et al. (2020) concentrated on improving the scheme’s efficiency and viability for real-world application, further developing cryptographic techniques to guarantee the anonymity and security of whistleblowers and investigating additional use cases and integration opportunities within various sectors. Sanz-Bas et al. (2021) highlighted the difficulties caused by the absence of a central regulatory body and the anonymity offered by cryptocurrencies, underscoring the complexity with which criminal groups are utilizing them for money laundering. To protect against potential fraud and improve the legitimacy and safety of such fundraising methods, Tiwari et al. (2020) called for further research into the risks associated with initial coin offerings (ICOs) as a new method of raising funds. They emphasized the need for in-depth investigation into the regulatory, operational, and security aspects of these methods. Dupuis & Gleason (2021) outlined a research agenda for the future that centers on recording the innovation cycle in cryptocurrency-related assets and exchange platforms as they develop in the context of money laundering, considering the authorities’ asymmetric reactions. To effectively combat emerging cyber threats, Broadhead (2018) proposed a comprehensive approach to understanding the dynamics of cybercrime through multidisciplinary studies, with a focus on the evolution and complexity of malware, the darknet, and cryptocurrencies within the cybercrime ecosystem. Additionally, the author emphasized the need for global cooperation and innovative cybersecurity strategies.

To present price manipulation in the crypto ecosystem, Gandal et al. (2018) underscored the necessity for exchanges to guard against fraudulent trading and suggested that despite increased market capitalization, the proliferation of cryptocurrencies creates more markets vulnerable to manipulation, underscoring the potential for continued manipulation risks in thinly traded markets. Phillips & Wilder (2020) called for further research into the operation of low-touch cryptocurrency scams, emphasizing the importance of developing automated identification and prevention techniques. This is aimed at enhancing the understanding and defense of the cryptocurrency industry against such scams, highlighting the dynamic and evolving nature of advance-fee scams and their operation across social media platforms. The research agenda outlined in Hornuf et al. (2022) pertains to future studies that delve more deeply into ICO fraud cases that have been deemed fraudulent or illegal by regulatory bodies such as the SEC. Additionally, new approaches to identifying fraud need to be investigated, such as comparing the content of white papers with verified firm facts, and the sources of fraud must be categorized, including whether they were intentional or the result of unforeseeable circumstances. Trozze et al. (2022) highlighted the need for more study into recently discovered cryptocurrency fraud areas and placed a high priority on stakeholder collaboration to address these new threats and improve the knowledge of and mitigation of these types of fraud.

In the systematic review performed by Kher et al. (2021), an outline for future research has been given that focuses on various phenomena, applicable theories, appropriate methodologies, and relevant data. The regulatory environment, corporate governance in crypto startups, the rise of cybersecurity industries to combat fraud, and the impact on traditional industries are some of the promising phenomena that can be investigated. Relevant theories to explain these phenomena include institutional theory, signaling theory, legitimacy theory, and transaction cost theory. Mackenzie (2022) presents a study agenda for the future that will be centered on comprehending how new technosocial dynamics and classic criminal behaviors interact inside cryptocurrencies and larger digital financial systems. This study highlights how important it is for criminology to adjust to and investigate the complicated, hybridized character of lives that are lived both offline and online, especially as society becomes increasingly interconnected and focused on the metaverse. This entails looking into the murky,
frequently unregulated cryptocurrency trading marketplaces, where fraud and manipulating the market have grown commonplace, and comprehending how these activities fit into the changing context of cybercrime. Using convenience theory, Almaqableh et al. (2023) established that for some cryptocurrencies, there are strong relationships between abnormal returns in the cryptocurrency market and drug trafficking activities. Future empirical research in this direction may reveal interesting insights into the cryptocurrency literature.

While examining the challenges of investigating ransomware attacks and other cybercrimes facilitated by cryptocurrencies, Irwin & Dawson (2019) emphasized the need for global regulation to address these issues. This study highlights three vital success factors for developing a global regulatory framework. The authors suggested that any attempt to develop a global regulatory framework may not be successful unless it can offer consistency, clarity, and cost-effectiveness. Opportunities exist for various stakeholders around the world to work toward developing a universal framework with such qualities. In an earlier study by Reynolds & Irwin (2017), it was suggested that even though crypto transactions offer anonymity, it is feasible for law enforcement agencies to trace illicit transactions if third-party collection of forms of identification is practiced backed by universal regulations that mandate identification standards supported by anti-money laundering and counterterrorism financing laws. Kethineni & Cao (2020) presented a more recent picture of the crypto landscape. They highlighted that cybercrimes spill over from the virtual world to the physical world, and the opposite often occurs. In most countries across the world, crypto transactions are not regulated well enough. Additionally, the political angle of crypto usage was pointed out in the study. Considering all the existing factors surrounding the crypto world, greater reporting of virtual currency-related crimes, well-rounded efforts toward universal regulation, etc., can shape a more optimized practice of cryptocurrency around the planet.

Based on the review and clustering of the relevant literature, this study highlights several challenges facing the crypto-crime scene and proposes research questions that can be asked in future research studies in this area. Table 6 outlines the challenges and proposed research questions.

7. Discussion and Conclusion

7.1. Discussion

This paper sheds light on the current research practices, nature, practice theories, and future directions of cryptocurrency scams by conducting a bibliometric and content analysis. The analysis covers 111 documents from the Scopus database from 2015 to 2023. Although cryptocurrency became popular with Satoshi Nakamoto's first research on Bitcoin creation in 2009, scams in cryptocurrency started to appear in 2011. Since 2018, the publication trend of revealing cryptocurrency frauds has started to increase with the introduction of the Ethereum platform as a Bitcoin competitor, the widespread adoption of blockchain technology in fintech, and the emergence of initial coin offerings (ICOs). 2018 is noted for its high number of scientific publications, with 21 publications on cryptocurrency scams. The steep increase in cryptocurrency research in 2018 suggests that more scams are receiving attention as cryptocurrencies become more popular with investors and regulators, and cryptocurrencies will emerge as fundamental research areas. Şcheau et al. (2020) stated that the popularity of cryptocurrency exploded after 2018 with the rise of fintech, as some fascinating niches in the literature focused on market efficiency, asset pricing bubbles, contagion, decoupling hypotheses, or volatility clustering. The author mentioned that the rise of cryptoconvuds coincided with failure in regulatory oversight, the potential for illicit use due to anonymity within an underdeveloped exchange system, and infrastructural breaches resulting from the growth of cybercriminal activities.

The number of publications has increased exponentially, with 95% in 2022 and 180% in 2023 compared to 2021. The reasons are tighter microeconomic conditions, more fintech innovation, the more complex nature of crypto crimes, the rise of decentralized markets, the fall of SVM, and investors betting on cryptocurrency. The results show that approximately 75% of our research sample has coproduced output, and 24% of the published papers have international collaborations. This shows that more collaboration with fellow researchers can expand the research scope and improve the quality of the work. At the same time, significant international collaboration among researchers from different parts of the world will bring diverse perspectives and ideas, contributing to the success of revealing more about cryptocurrency fraud. In the case of the most influential cited articles, the top two journals are concentrated on ransomware and cybersecurity. The top 10 cited articles focused on criminal activities in money laundering and the Ponzi scheme and the use of the dark web for cash-out strategy as an anonymous identity and highlighted the challenges and importance of regulatory actions and law enforcement to prevent crypto scams. After the introduction of the organized cryptocurrency trading market, there were signs of building financial pyramids, and criminals found new opportunities for money laundering. Hendrickson & Luther (2022), Baroletti et al. (2018), Rivera (2019) and Hendrickson & Luther (2022) countries that go cashless are not less vulnerable to money laundering. Instead, they offer greater financial anonymity, allowing transactions with lower detection risk than traditional digital payments.
The top 10 journals contributed more than 1000 citations, each with an average of 105 citations. Universities from the UK and Australia published the most research on Cryptocurrency scams. In addition, there was a significant increase in research publications in 2020, with many prestigious institutions contributing to the field. The University College of London published the most research articles on cryptocurrency scams in a single year, with 7 papers published in 2022 and 8 papers in total. It shows the level of expertise and dedication of the researchers at the university in this field. The top-ranked

Table 6 Challenges and Proposed Research Questions.

<table>
<thead>
<tr>
<th>Clusters</th>
<th>Challenges</th>
<th>Proposed Research Questions (PRQs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptocurrency in illegal activities, regulatory challenges, and legal consequences</td>
<td>1. Unraveling cryptocurrency’s role in illegal activities</td>
<td>PRQ1. How can effective monitoring mechanisms be developed to detect the use of cryptocurrencies in illegal activities, while respecting privacy and legal boundaries?</td>
</tr>
<tr>
<td></td>
<td>2. Addressing insufficient regulations for crypto misuse prevention</td>
<td>PRQ2. What regulatory frameworks can be established or amended to effectively govern the use of cryptocurrencies and prevent their misuse in crimes?</td>
</tr>
<tr>
<td></td>
<td>3. Challenges in monitoring advanced crypto mechanisms</td>
<td>PRQ3. How do law enforcement and legal systems adapt to the challenges posed by the global and decentralized nature of cryptocurrency transactions in the context of illegal activities?</td>
</tr>
<tr>
<td></td>
<td>4. Navigating legal consequences and cross-border issues in crypto crimes</td>
<td></td>
</tr>
<tr>
<td>The crypto ecosystem and the dual nature of crypto usage</td>
<td>1. Prevalence of fraud and scams in cryptocurrency transactions.</td>
<td>PRQ1. How can fraud and scams in cryptocurrency transactions be more effectively identified and prevented?</td>
</tr>
<tr>
<td></td>
<td>2. Complexity in identifying and tracing cryptocurrency fraud.</td>
<td>PRQ2. What methods can improve the tracing and accountability of cryptocurrency fraud?</td>
</tr>
<tr>
<td></td>
<td>3. Vulnerability of cryptocurrencies to price manipulation.</td>
<td>PRQ3. How can the cryptocurrency market be safeguarded against price manipulation?</td>
</tr>
<tr>
<td></td>
<td>4. Challenges in distinguishing between legitimate and fraudulent ICOs.</td>
<td>PRQ4. What criteria can be established to differentiate between legitimate and fraudulent ICOs?</td>
</tr>
<tr>
<td></td>
<td>5. Difficulties in regulating and monitoring cryptocurrencies due to their decentralized nature.</td>
<td>PRQ5. How can regulatory frameworks adapt to effectively monitor and control the decentralized nature of cryptocurrencies?</td>
</tr>
<tr>
<td></td>
<td>6. Dual nature of cryptocurrencies, used for both legitimate and illicit purposes.</td>
<td>PRQ6. How can the legitimate use of cryptocurrencies be maximized while minimizing their use in criminal activities?</td>
</tr>
<tr>
<td>Societal effects of tech innovation and interdisciplinary research need in criminology, economics, computer science for tech challenges</td>
<td>1. Gaps in interdisciplinary research on cryptocurrencies.</td>
<td>PRQ1. How can interdisciplinary research in criminology, economics, and computer science contribute to understanding the societal impacts of cryptocurrencies?</td>
</tr>
<tr>
<td></td>
<td>2. Broad societal effects of cryptocurrency technology.</td>
<td>PRQ2. What are the broader societal implications of the adoption of cryptocurrency technologies?</td>
</tr>
<tr>
<td></td>
<td>3. Cryptocurrency’s role in the wider economic system.</td>
<td>PRQ3. How do cryptocurrencies integrate into and impact the global economic system?</td>
</tr>
<tr>
<td></td>
<td>4. Ethical and legal implications of cryptocurrency use.</td>
<td>PRQ4. What legal and ethical frameworks are needed to govern the use of cryptocurrencies?</td>
</tr>
<tr>
<td></td>
<td>5. Cryptocurrency tech outpacing policy frameworks.</td>
<td>PRQ5. How can policy and regulatory frameworks evolve with the rapid technological advancements in cryptocurrencies?</td>
</tr>
<tr>
<td>Tracing crypto footprint in illegal activities.</td>
<td>1. Anonymity in cryptocurrencies hinders transaction tracking.</td>
<td>PRQ1. What new methods and technologies can be developed to improve the tracing of cryptocurrency transactions in illegal activities?</td>
</tr>
<tr>
<td></td>
<td>2. Cryptocurrency tech outpaces forensic methods.</td>
<td>PRQ2. How can the balance between user privacy and the need for security and transparency in cryptocurrency transactions be achieved?</td>
</tr>
<tr>
<td></td>
<td>3. Cryptocurrency privacy features obstruct user identification.</td>
<td>PRQ3. What role can interdisciplinary research play in developing more effective strategies for tracking illegal cryptocurrency transactions?</td>
</tr>
<tr>
<td></td>
<td>4. Cryptocurrency’s global, decentralized nature complicates legal jurisdiction.</td>
<td>PRQ4. How can international cooperation be improved to address the cross-border nature of cryptocurrency crimes, and what changes in legal frameworks are needed?</td>
</tr>
<tr>
<td></td>
<td>5. Mainstream cryptocurrency uses obscures tracing of illegal activities.</td>
<td>PRQ5. How can law enforcement agencies and regulatory bodies adapt their strategies to keep pace with the rapid evolution of cryptocurrency technologies?</td>
</tr>
<tr>
<td></td>
<td>6. Need for standardized cryptocurrency forensic tools and methods.</td>
<td>PRQ6. What are the best practices and standards that can be developed for cryptocurrency forensic investigations?</td>
</tr>
</tbody>
</table>
Research institutions are from England, Australia, the United States, the Czech Republic, the UAE, China, South Korea, and Saudi Arabia. We found that the research funding of the top ten universities also focuses on government subsidies, lab research funding, fellowships, private partnerships, and other sources of similar findings. Universities from both developed and developing countries are showing a keen interest in producing articles on cryptocurrency-based scams research. The USA is the most significant contributor to cryptocurrency scam research, with 10 publications and 567 citations, followed by the UK, with 9 papers and 187 citations. Among all countries, the USA has shown a steep increase in the number of articles published consistently over the years. Irwin and Dawson (2019) studied the appropriate regulation of payment methods in developed countries. According to them, a globally practical regulatory framework remains a distant reality; it is noteworthy that countries such as Australia, Canada, the UK, and the USA have emerged as leaders in complex and challenging regulatory spaces. Despite the difficulties involved, these countries have made significant progress toward creating a regulatory framework that effectively addresses financial crimes while fostering innovation and growth. China, the UAE, Indonesia, and Saudi Arabia are showing overwhelming concerns about research in Asia. Interestingly, although developing countries have contributed much more to research on crypto scams, publications from developed countries have been cited significantly. This indicates that research from developed countries has great value and research potential in the future. It is worth noting that research publications from developed countries, such as the UK, Australia, Germany, and the Netherlands, are highly concentrated within national boundaries. Scholars in developed countries are heavily involved in researching cryptocurrency, but there needs to be more collaboration with other researchers worldwide. It would be valuable to see more global cooperation in this field to gain a broader understanding of these financing models. Many collaborative approaches have been found between the USA and the UK, between the USA and China, and between Australia and Canada. The other countries maintaining a steady collaborative network include China, Canada, the UAE, the Netherlands, and Indonesia. The Journal of Money Laundering and Control was the top contributing journal in this research area and accounted for 9 articles. Among these sources, Computers and Security had the greatest number of citations (333). Among researchers, Gleason K., affiliated with the American University of Sharjah, United Arab Emirates, and Kleinberg B., affiliated with Tilburg University, Netherlands, are the most contributing authors, accounting for 3 papers each. Kleinberg B. is at the top of the list regarding influential research on cryptocurrency scams and has the highest number of 121 citations.

The analysis of the relevant research on cryptocurrency and related crimes reveals remarkable tendencies and clusters—cryptocurrency and Bitcoin dominate, representing 35% and 16% of total frequencies, respectively. Recent research areas include crimes involving electronic money, malware, and ransomware. In 2018–2023, the emphasis shifted from malware, bitcoin, and blockchain to fintech-based crimes such as money laundering, pump-and-dump schemes, and phishing. Researchers organize keywords into groups, emphasizing themes such as blockchain’s function in anti-money laundering, bitcoin’s relationship with ransomware, virtual currency legislation, and cryptocurrency fraud. The interdisciplinary nature of the research, which includes technology, law, finance, and cybersecurity, emphasizes the complexities of tackling issues at the junction of cryptocurrency and financial crimes. Cryptocurrency research has focused on the facets of crypto crimes, such as money laundering, cybercrime, digital forensics, and regulation, as evidenced by thematic maps. Researchers should emphasize anti-money laundering, cybercrime, digital forensics, and cybersecurity since they can benefit the field (Higbee, 2018; Kfir, 2020; Dolejška et al., 2023). According to the factorial analysis, the topics surrounding cryptocurrency crimes, such as money laundering, financial crime, fraud, and digital forensics, are interconnected. A comprehensive study of these topics might contribute to combating the threats of criminal activities in cryptos.

Co-citation analysis revealed that the work of Nakamoto, Smith, Moore, McCoy, and Corbet is closely linked to that of the other clusters and fellow cluster companions. Bibliographic coupling revealed four thematic clusters. These included using cryptocurrencies in illicit activities, regulatory challenges, the societal impacts of technological innovations such as blockchain, and difficulties in tracking the cryptocurrency footprint in illegal activities. A common theme across these clusters was the urgent need for improved regulatory and legal frameworks to address the challenges in the rapidly evolving digital financial arena and mitigate cryptocurrency-related crimes (Dupuis & Gleason, 2020; Hornuf et al., 2022, Irwin & Dawson, 2019). Cryptocurrency has become a popular platform for wide-ranging criminal activities, posing financial threats to investors and users while providing a sanctuary for scammers, fraudsters, and criminals. ICO fraud, money laundering, Ponzi schemes, phishing, darknet market transactions, ransomware, pumps and dumps, exchange scams, and corruption are some of the predominant crimes in crypto. Despite the efforts of lawmakers to establish laws to make cryptocurrencies safer investment vehicles, criminals devise new types of fraud, making it difficult for regulators to catch up (Sanz-Bas et al., 2021). The reasons for cryptocurrency crime are illustrated using relevant theories. The link between relevant theory and reasons for emerging crypto-crimes is that rational choice theory highlights reasons such as anonymity, decentralization, lack of regulations, and investor overconfidence; convenience theory explains reasons such as decentralization, anonymity, low barriers to entry, lack of regulations, access, and ease of conversion; and social learning theory states that speculative expectations, investor overconfidence, anonymity, lack of regulations and space transition theory speaks about decentralization, lack of regulations, access, ease of conversion, low barriers to entry and speculative expectations.

We also outline a comprehensive future research agenda aimed at addressing the various challenges related to ransomware attacks, blockchain-based reporting schemes, cryptocurrencies in illegal activities, initial coin offerings (ICOs),
and so on. This highlights the need for improved user awareness, enhanced security and anonymity for whistleblowers, and the investigation of cryptocurrencies’ role in money laundering and fundraising fraud. The agenda also emphasizes exploring the innovation cycle in cryptocurrency assets, understanding cybercrime dynamics, guarding against crypto market manipulation, and developing automated scam prevention. Moreover, it suggests studying the socioeconomic impacts of cryptocurrencies, the necessity for standardized global regulation, and the integration of interdisciplinary research to tackle tech challenges in criminology, economics, and computer science. In addition, we have proposed specific research questions focused on monitoring illegal crypto-activities, regulatory frameworks, fraud identification, societal effects of tech innovation, and the development of new forensic tools aimed at safer and more regulated crypto-ecology and environment.

7.2. Implications of the study

Scammers often promote fraudulent investments in new cryptocurrencies to hide the funding source by using crypto exchange loopholes or exploiting vulnerabilities in digital wallets. Although developed countries are hotspots of crypto-economics and a series of high-profile scams, the adoption of cryptocurrency is flourishing in developing countries. As a result, it is imperative to conduct more research and exchange proper policy guidelines to prevent underworld activities such as buying drugs, guns, and other illegal goods in the cryptocurrency ecosystem. Moreover, countries with research barriers to unveiling cryptocurrency scams and lower government infrastructure support can collaborate with professional crime experts and researchers for faster adoption of prevention measures. Recognizing outstanding scholars, publication trends, and affiliated institutions and identifying emerging themes and publishers can be beneficial for researchers and academics. This can help learn from best practices, ensuring safe and secure digital asset transactions and producing better strategic and regulatory outcomes than expected. However, we noticed that cryptocurrency-related fraud and criminal activities are still growing, an effective balance between potential benefits and risks for cryptocurrency circulation remains unanswered, and adopting safe and secured virtual currency in a regulated decentralized financial network to combat criminal activity remains unpredictable. Practitioners can use bibliometric analysis and future actions to gain actionable insight, tracking the viability of an effective risk-oriented approach and the propensity of digital fraud schemes in the long term rather than staying in the illusion of having a uniform digital coin sooner or considering cryptocurrency equivalent to traditional fiat currency. Regulators and policymakers can leverage research findings in developing a framework that promotes responsible risk-taking behavior and safeguards potential fraud victims. Financial crime professionals can also leverage this discussion of research theories and questions to identify the vulnerability of individuals to crypto-fraud schemes and formulate adequate regulations to mitigate risks while fostering innovation.

7.3. Limitations and Future Study

This study considered only the Scopus database, and the inclusion criteria were focused on economics, finance, and business settings. However, these studies can be broadened to different fields and extended to the Web of Science database. Second, this study focused on financial crime and did not consider any nonfinancial scams or frauds in the analysis. Future studies can be extended to the psychological understanding of cryptocurrency fraud, consumer trust in cryptocurrency, and the classification of cryptocurrency fraud based on geographical positions and fintech-based cryptocurrency fraud.

Ethical Considerations

Not applicable.

Conflicts of Interest

No conflicts of interest.

Funding

This study received no funding.

References


