Scientometrica 2 (2026) 65–82

Contents lists available at GrowingScience

Scientometrica

homepage: www.GrowingScience.com/sci

# Exploring the landscape of cryptocurrency and security research: A bibliometric study enhanced by LLM-based affiliation harmonization

**Manju Bhardwaj[a], Shweta Sankhwar[a], Ojasvi Yadav[a], Rinkal Bhadauria[a], Sushila Madan[b] and Shikha Badhani[a*]**

[a]*Department of Computer Science, Maitreyi College, University of Delhi, Delhi, India*
[b]*Department of Computer Science, Lady Shri Ram College, University of Delhi, Delhi, India*

**C H R O N I C L E**

*Article history*:
Received: January 21, 2026
Received in revised format: January 29, 2026
Accepted: January 31, 2026
Available online:
January 31, 2026

*Keywords:*
*Cryptocurrency*
*Security*
*Bibliometric*
*Scopus*
*Web of Science (WoS)*
*Large Language Model (LLM)*

**A B S T R A C T**

Over the past decade, decentralized digital currencies have gained prominence in finance and technology, but their growth has also drawn adversaries exploiting security vulnerabilities. This paper reviews the literature on cryptocurrency and security using bibliometric analysis of Web of Science and Scopus articles published between 2013 and May 2025. Tools such as Biblioshiny and VOSviewer were employed to explore key trends, influential contributors, collaborative networks, and emerging themes. A novel contribution of this study is the use of Large Language Models (LLMs) to address inconsistent affiliation formats, enabling accurate identification of leading academic organizations. The results demonstrate that LLM-based harmonization effectively prevents misrepresentation in bibliometric datasets. Overall, this study not only summarizes evolving research trends in cryptocurrency and security but also highlights the potential of LLMs to enhance bibliometric methods, suggesting broader applications for improving the accuracy and reliability of future scholarly analyses.

© 2026 by the authors; licensee Growing Science, Canada.

## 1. Introduction

In the fast-paced, technology-driven world we live in today, there are always new opportunities to learn, think about, and put into practice. Initially, we marveled at the convenience of paying bills with a simple phone click instead of visiting a bank. However, as time progresses, new phenomena emerge, and we find ourselves grappling with concepts like “Digital Currency” or “Cryptocurrency”. The foundational concept of cryptocurrency was rooted in the invention of the "Blinding Algorithm" in the 1980s, establishing the fundamental principles of this technology (Chaum 1983). Subsequently, on April 21, 1990, the concept of electronic cash took a significant step forward with the introduction of “digicash”. This pioneering step aimed to assuage concerns surrounding online buying and selling (Chaum et al., 1990). Building upon this progress, the year 2008 marked a watershed moment when an enigmatic figure or group operating under the pseudonym "Satoshi Nakamoto" introduced the world to the concept of bitcoin (Nakamoto, 2008). In 2008, the rise of Bitcoin introduced the term cryptocurrency to the general public. Bitcoin was designed as a protocol to allow a network of individuals to issue digital tokens and transfer them among themselves using peer-to-peer digital communications infrastructure while maintaining security through cryptography (Nakamoto 2008). Although the original proposal did not use the term cryptocurrency, Nakamoto referred to the project as a peer-to-peer currency in a network and cryptography mailing list (Nakamoto, 2008). Cryptocurrencies like Bitcoin rely on blockchain, which is a series of interconnected blocks that can be thought of as a public ledger where all committed transactions are recorded. When further blocks are added to the chain, it continues to grow (Zheng et al., 2018).

* Corresponding author.
E-mail address: shikhamalik2@gmail.com (S. Badhani)

ISSN 3115-8455 (Online) - ISSN 3115-8447 (Print)
© 2026 by the authors; licensee Growing Science, Canada
doi: 10.5267/j.sci.2026.3.001

Blockchain technology is widely recognized as a highly promising innovation, boasting potential applications across diverse industries such as finance, security services, non-fungible tokens (NFTs), logistics, and supply chain management. Among its various applications, the most renowned is its pivotal role in enabling cryptocurrencies. At its core, blockchain serves as an exchange medium akin to traditional money. Importantly, cryptography is integrated into the exchange process, safeguarding financial operations, validating asset transfers, and regulating the creation of new units (Isaac Christopher 2022). This technology provides a secure platform, a fact that has led numerous organizations around the world to embrace it. In the realm of cryptocurrency transactions, blockchain technology has established a resilient digital ledger that largely acts as a deterrent to hackers. Nevertheless, this does not render it impervious to cyberattacks. Notably, within the cryptocurrency market, unlike in the traditional banking sector, any lost funds are irrecoverable.

The fact that all operations related to this cryptocurrency occur online inherently gives rise to security concerns, malware attacks, and illicit transactions, among other risks. In an environment centered around money, there will invariably be individuals seeking to exploit it. Furthermore, in the absence of government authority, the protective umbrella of government oversight is absent. All developers of cryptocurrencies are actively working towards enhancing the security aspects. Given the rapid pace of developments and emerging risks in cryptocurrency and security, bibliometric analysis serves as a valuable method to track research progress, synthesize existing knowledge, and support informed strategic decisions of researchers and stakeholders (Donthu, Kumar, Debidutta Mukherjee, et al., 2021). In various studies (Navamani 2023; Conti et al., 2018; Lim et al., 2014; Pandya et al., 2019), the security aspect of cryptocurrency has been covered. But to the best knowledge of the authors, no study has focused on the bibliometric analysis of the security aspect of cryptocurrency in a single article. To fill this gap, we have conducted a formal study that not only highlights the current state of the art but also outlines future directions in this domain thus proving to be an intriguing research pursuit. Moreover, the scope of this study is adequately large to warrant a method such as bibliometric analysis that can handle large volumes of bibliometric data (Ramos-Rodríguez and Ruíz-Navarro 2004).

In this paper, we employ bibliometric analysis to comprehend research trends in the area of cryptocurrency and security. Bibliometrics is a statistical method for analyzing publications that offer quantitative insight into the body of academic literature (De Bellis 2009). Bibliometric analysis illuminates the evolution of literature and the dissemination of information over time within a given field. This is achieved through the analysis of data derived from databases, encompassing citations, authors, keywords, and the selection of consulted journals (Van Raan 2005). Depending on the information it analyzes, bibliometric analysis uses a variety of approaches, including performance analysis that presents the performance of research constituents such as authors, institutions, countries, journals, etc. in the field under consideration, and science mapping that includes citation analysis, co-citation analysis, bibliographic coupling utilizing citations (De Bellis 2009), co-word analysis using keywords (He 1999), and co-authorship analysis, which examines the relationship between research constituents (Ramos-Rodríguez and Ruíz-Navarro 2004). Also, these basic techniques can also be augmented with network metrics, clustering, and visualization techniques to enrich the results of the analysis (Donthu, Kumar, Debmalya Mukherjee, et al., 2021).

A preliminary bibliometric analysis on general cryptocurrency research was conducted as a pilot study to identify thematic gaps. This served as a foundational step toward a more targeted bibliometric investigation into cryptocurrency and security. This study performs a systematic and quantitative bibliometric analysis of cryptocurrency and security literature in top journals and articles related to these topics and related important keywords. Among the available bibliometric databases, Scopus and Web of Science (WoS) were selected for their broad and complementary coverage. Utilizing both the databases enhances the completeness and balance of the analysis by reducing disciplinary and regional biases (Mongeon and Paul-Hus 2016). Since in this study we intend to provide a review of the past, present, and future of the area of cryptocurrency and security, we have employed the performance analysis along with co-citation analysis, bibliometric coupling, and co-word analysis to reveal and visualize a bigger picture and evolution of this research area. Furthermore, this study also addresses the known issue of inconsistent affiliation formats that may result in inaccurate identification of the top organizations. To overcome this limitation, we employed a Large Language Model (LLM) to standardize and harmonize affiliations along with a carefully drafted instruction prompt. The results were validated to ensure the reporting of accurate top institutions for bibliometric analysis.

The contributions of this paper are manifold. First, by utilizing the bibliometric technique, this study can assist researchers in analyzing particular fields in the extant literature on cryptocurrency with large bibliometric data and corpus. Second, this study not only validates its aim of working on the security aspect of cryptocurrency but also lays strong foundations for advancing in a field in new and significant ways by identifying knowledge gaps that generate novel ideas for future research. Lastly, a novel use case of employing LLMs for bibliometric analysis is presented.

The rest of the paper is structured as follows. The paper begins with a review of prior work in the areas of cryptocurrency and bibliometric analysis followed by the methodology. The subsequent section presents the findings from the bibliometric analysis and highlights key insights. The paper concludes with a summary of contributions and key takeaways.

## 2. Literature Review

In this section, we present a review of works which either evaluate security measures adopted for cryptocurrency or perform bibliometric analysis.

### *2.1. Cryptocurrency and Security*

Although cryptocurrency is difficult to forge, it's massive growth has made it a soft target for competitors who have identified the vulnerabilities of the system and hence induce attacks like double spending and networking attacks. Various research papers perform an evaluation of the security and protection measures for cryptocurrencies, especially for Bitcoin (Navamani 2023; Islam et al., 2021; Conti et al., 2018). The survey conducted by Conti *et al.* (Conti et al., 2018) revealed that while the development of the Bitcoin protocols with proof-of-work and consensus to protect user actions are the robust features of Bitcoin, these are themselves turning into a point of manipulation for cyber thieves. Islam *et al.* (Islam et al., 2021) analyzed the Bitcoin protocol and identified potential vulnerabilities and attacks such as double spending and Sybil attacks. They also discuss the privacy concerns associated with Bitcoin and propose solutions to address these issues. Navamani (Navamani 2023) examined 80 research publications to study the notion of blockchain ecosystems, the split of blockchains, the implementation of blockchains, and lastly security concerns and blockchain issues.

Unlike these earlier studies, which primarily offer qualitative summaries and theme discussions, our research use bibliometric analysis to examine the cryptocurrency and security domain. In this study, we examine publication patterns, key contributors, collaboration networks, and emerging areas of interest to offer a clear, data-driven picture of the evolution of this field of study and its future directions.

### *2.2. Bibliometric Analysis*

In 1969, Pritchard (Pritchard 1969) coined the term "bibliometrics" as "the application of mathematical and statistical approaches to books and other forms of communication". Bibliometrics is used to examine the trends of publishing within a discipline, and employ quantitative analysis of empirical data in published literature. Thus, it helps a researcher to identify the major topics in their area of study. To see the intellectual structure, bibliometric analysis, and science mapping methodologies are frequently used together (De Bellis 2009; Al-Ali et al., 2025; Al-Raggad 2025). Depending on the type of information utilized in the studies, bibliometrics performs a variety of analysis such as citation-based analysis, co-word analysis or keyword co-occurrence analysis, and co-authorship analysis(Sarkar et al., 2020).

According to Nasir *et al.* (Nasir et al., 2021), bibliometric analysis performed on 1965 documents during the analysis period (2015-2020), draws attention to the conceptual and impactful features of blockchain and cryptocurrency literature. With the help of a co-occurrence network, they suggest three main research streams of available publications: cryptocurrency structure and blockchain technology implications; privacy, security management of data and information; and creation of ideal information systems. Another bibliometric analysis study in the area of blockchain was performed Guo *et al.* (Guo et al., 2021). The data for the study was gathered from the *Web of Science* core collection. Data was gathered from 3826 papers that were published between 2013 and 2020. The publishing patterns and categories, in particular, may shed information on the development trends and active areas of blockchain research. This findings of this bibliometric analysis suggest that the theoretical understanding and popular blockchain research subjects mostly focused on "smart contracts", "bitcoin", "security", "ethereum", and "cryptography" (Guo et al., 2021). Both of the above bibliometric analysis studies pointed towards exploring more about the security aspect of cryptocurrency. In (Yuan et al., 2022), bibliometric analysis of blockchain security research between 2014 to 2020 from WoS database is presented. One of the main finding was the identification of key research hotspots that include cryptocurrency, smart contracts, cyber attacks, IoT, and consensus mechanisms.

Our study combines information from the WoS and Scopus databases, thereby eliminating selection bias and offering a more thorough picture of the state of security and cryptocurrency research. Moreover, our study covers a wider range of cryptocurrency security, including many facets outside of blockchain, whereas Yuan et al. (Yuan et al., 2022) concentrate exclusively on blockchain security.

## 3. Methodology

The methodology of this study is shown in Fig. 1 that is elaborated in the subsections below.

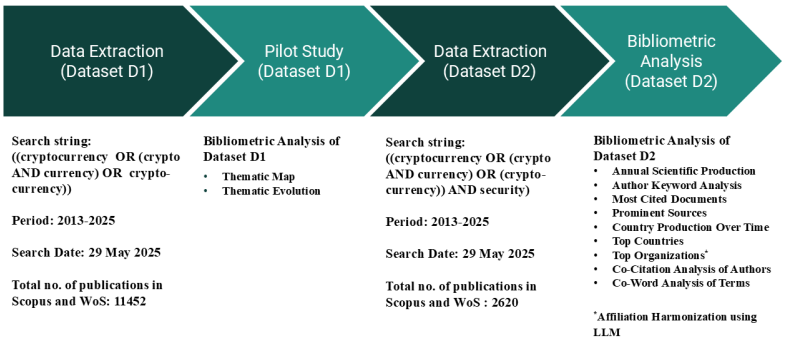


**Fig. 1.** Methodology

### *3.1. Tools for Bibliometric Analysis*

The tools used for the bibliometric analysis of the data in this study were:

1. Bibliometrix R package (www.bibliometrix.org) (Aria and Cuccurullo 2017), an open-source comprehensive tool for bibliometric analysis was used. The analysis leveraged both the core R scripting functionalities and the Biblioshiny web interface , which facilitates interactive exploration, visualization, and customization of bibliometric data. It is excellent for creating stunning and engaging visualisations and is a fantastic tool for finding patterns in a dataset.

2. Bibliometric networks were built and visualized using VOSviewer (www.vosviewer.com) (Van Eck and Waltman 2014). VOSviewer is a widely used tool in literature for performing bibliometric analysis.

3. Ollama (www.ollama.com) (Ollama 2023) + LLaMa 3:8B (www.ollama.com/library/llama3) (LLaMA Team 2024), a locally run large language model framework, was used to extract and harmonize institutional affiliations for organization-level insights.

### *3.2. Data Collection*

Peer-reviewed literature from the Scopus (Scopus 2025) and WoS (Web of Science 2025) databases (recognized as the greatest repositories of peer-reviewed literature (Aghaei Chadegani et al., 2013)) were searched with the primary goal of examining security in cryptocurrency.

To investigate the thematic landscape and determine whether a concentrated study on Cryptocurrency and Security was necessary, a preliminary bibliometric examination of the larger field of cryptocurrency was carried out. Firstly, all the data were downloaded for the search result of the query string (search date: 29 May 2025) in the Title-Abstract-Keyword column of *Scopus* and *WoS* databases: (cryptocurrency OR (crypto AND currency) OR crypto-currency), which reported 12989 matches on *Scopus* and 3694 on *WoS*, starting from the year 2013. The inclusion criteria for this study were confined to articles, conference proceedings papers, and reviews. In addition, only documents written in English were considered. Conference papers that were later extended to journal articles were excluded. Finally, after merging data from Scopus and WoS results, duplicates were removed to obtain the final Dataset D1 consisting of 11449 documents. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines (Page et al., 2021) were employed to select and screen documents for the final bibliometric analysis, as illustrated in Fig. 2.

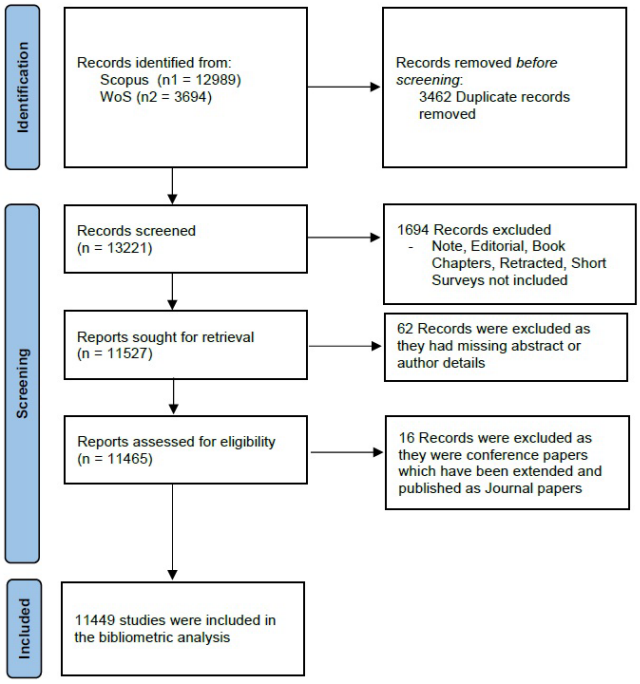


**Fig. 2.** PRISMA flow diagram for Dataset D1

A pilot study was conducted using bibliometric analysis on Dataset D1 with the Biblioshiny package in R. The analysis revealed that security in cryptocurrency studies had been underexplored, highlighting a clear research gap. This observation established a compelling rationale for conducting a focused investigation into the intersection of cryptocurrency and security

particularly for investigating past research trends in security and subsequently delving into the areas where this aspect was deficient or lacking. Consequently, dataset D2 was compiled which consisted of publications containing the term "Security" in Keywords, Abstract, or Title of publication.

Subsequently, all data were downloaded from *Scopus* and *WoS*, for the search results of the query string: (cryptocurrency OR (crypto AND currency) OR (crypto-currency) AND security), resulting in Dataset D2 comprising of 3042 matches in *Scopus* and 445 in *WoS*, between the year 2013 and 2025. Further after performing the PRISMA framework on D2, similar to that for D1, 2620 documents were finally selected as illustrated in Fig. 3. The data about publications resulting from both the aforementioned queries were exported in CSV files.

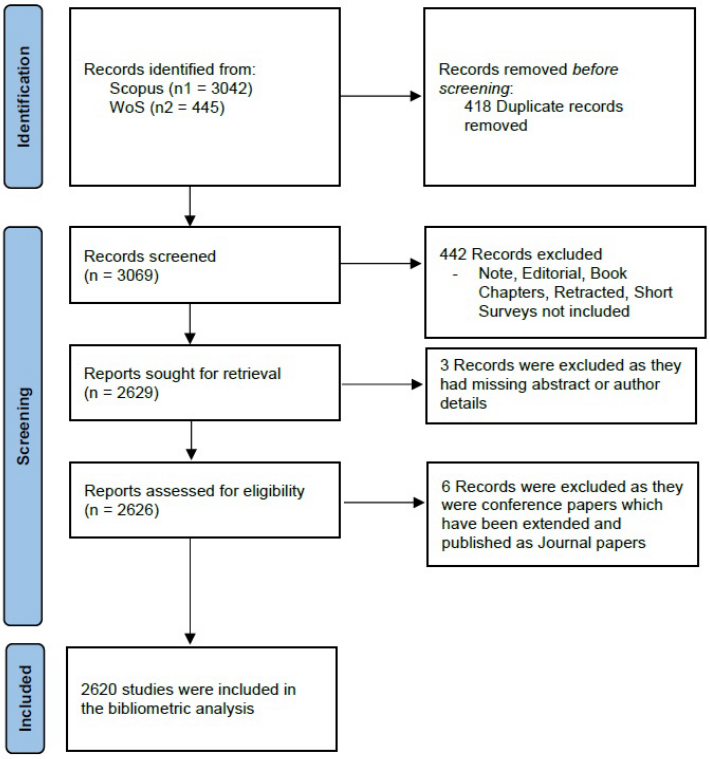


**Fig. 3.** PRISMA flow diagram for Dataset D2

## 4. Results and Discussion

In this section, we present the results after performing a bibliometric analysis on datasets D1 and D2.

### *4.1. Pilot Study on Dataset D1*

In this section, we describe the results of the pilot study performed to narrow down the different aspects of cryptocurrencies as evident in the literature. By exploring a broader dataset initially (Dataset D1), we were able to uncover promising trends that allowed us to refine the research questions and tailor hypotheses for the subsequent focused study. This strategic narrowing of the research scope significantly improved the value of the findings and insights generated in the smaller-scale study.

#### *4.1.1. Thematic Map*

A thematic map is used to learn about the current state of a study field and the potential of future research development of thematic areas within a field. The evolution of a study field can thus be captured using a thematic map. A thematic map divides the two-dimensional graph into four cluster quadrants, each representing a research subject or community of ideas within the discipline. Network features such as centrality and density are used to represent the evolutionary stage of each topic based on the location of the clusters (Muñoz-Leiva et al., 2012). Density represents the cohesiveness among the nodes while centrality measures the degree of linkage between various topics (Esfahani et al., 2019). These two characteristics assess a topic's importance and degree of development. A node's centrality and relevance increase along with the number of relationships it has with other nodes in the thematic network, placing it in a vital position. Similar to this, a research field's ability to grow and sustain itself is defined by the cohesion of the nodes that make up its density. In the thematic map, density is depicted along Y-axis, and centrality along the X-axis. The bubble size of each thematic cluster indicates

the prominence of the theme in the corpus of extant literature by reflecting the number of documents associated with each cluster.

The position of a cluster in a strategic diagram can be stated as follows: The upper right quadrant (I) represents the highest density and importance of the topics to the review field. These mainstream clusters account for the vast majority of research conducted during the time period under consideration. The upper left quadrant (II) has a high density of themes but insignificant external linkages (low centrality), indicating that they are of limited domain value. The clusters in this quadrant are specialized and distinct from the main area. Quadrant three (III) (bottom left) is in flux, with clusters indicating either emerging or waning themes. The fourth quadrant (IV) (lower right) comprises clusters of centrality that have not yet formed and have the potential to grow (Melcer et al., 2015).

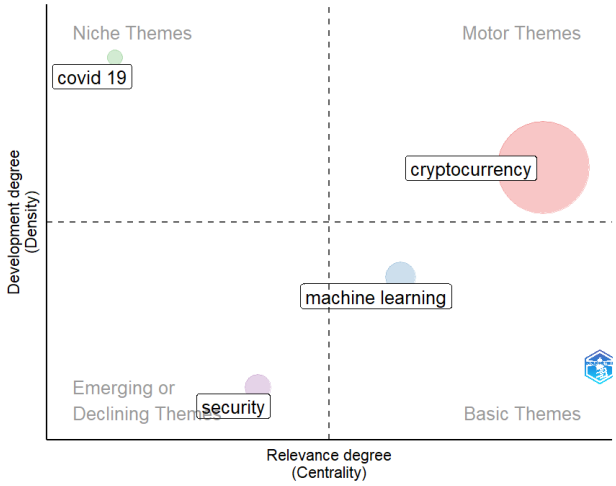


**Fig. 4.** Thematic map of Cryptocurrency (Dataset D1)

Fig. 4 shows the thematic map for the dataset D1 created via Biblioshiny web interface. It is clearly visible that *cryptocurrency* being the seed keyword, appears in the motor theme quadrant (I) with a large bubble size, underlining its position as the central, well-developed notion in D1. *Covid-19* appears in the niche theme quadrant (II) suggesting despite being well structured and cohesive, it exhibits limited connectivity to the central research area due to its low centrality. This is explained by the fact that numerous studies on the effects of the COVID-19 pandemic on cryptocurrencies were carried out in reaction to it, but this resulted in the development of a specialized subdomain. The basic theme quadrant (IV) focusing on *Machine learning* demonstrates a low level of thematic development, despite the high centrality. *Security* is in the emerging or declining theme quadrant (III) which implies low centrality and low density. To get further clarity about its emerging or declining status, we observe the occurence of keyword *security* in cryptocurrency publications. Fig. 5 shows the year-wise frequency of the keyword *security* in the cryptocurrency related publications. The strong rising trend of the keyword since 2017, supports its classification as an emerging theme within the cryptocurrency research landscape. Despite its minor thematic presence as indicated by the size of the bubble, this analysis draws attention to a crucial knowledge gap. To address this gap, we perform a targeted bibliometric analysis on the terms "cryptocurrency" and "security" in Sec. 4.3 to identify important contributions, new trends, and possible lines of inquiry.

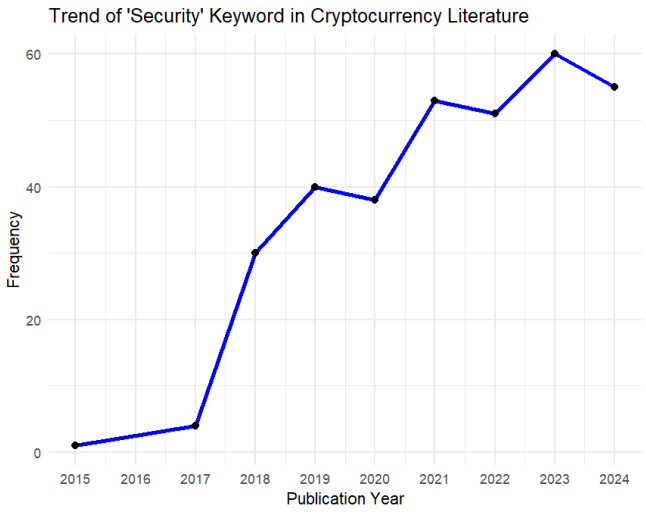


**Fig. 5.** Year-wise frequency trend of the keyword security in cryptocurrency-related publications.

### *4.1.2. Thematic Evolution*

The thematic evolution diagram created by using the Bibliometrix R package is presented in Fig. 6. It provides a complete overview of the conceptual evolution of cryptocurrency research from 2013 to 2025. The analysis is organized into four distinct temporal intervals, each depicting the dominant and emergent themes through keyword clusters, with arrows denoting conceptual inheritance and their thickness signifying the strength of continuity.

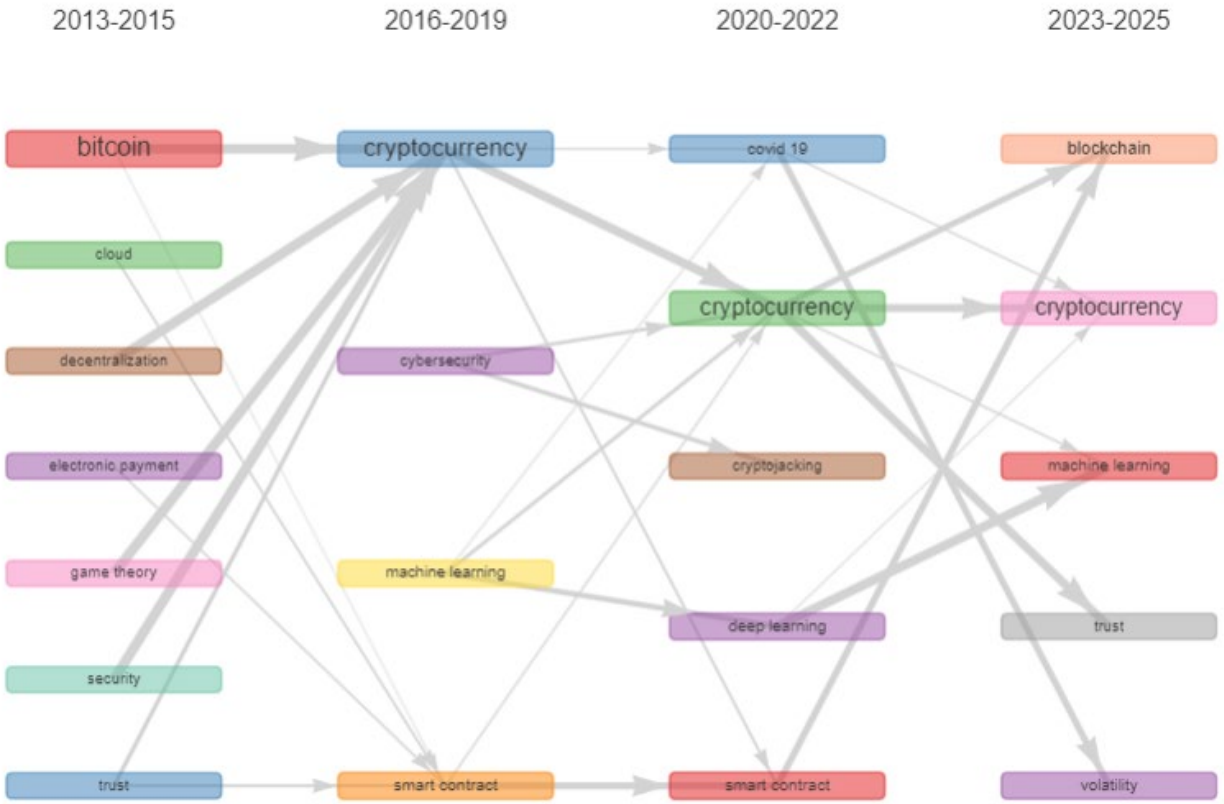


**Fig. 6.** Thematic evolution of cryptocurrency literature from 2013 to 2025.

The initial phase (2013-15) is dominated by foundational terms like bitcoin, security, and trust. The second phase (2016–2019) marked the expansion of the research landscape, with the emergence of themes such as cybersecurity, machine learning, and smart contracts signifying the onset of interdisciplinary areas. The third phase (2020–2022) demonstrates further specialization, with the appearance of *cryptojacking* and *deep learning*, indicating growing attention to targeted security threats and predictive technologies. Nevertheless, by the years 2023 to 2025, the notable lack of *security*-focused themes as predominant clusters—despite the rise of *blockchain*, *volatility*, and *trust*—underscores a fragmentation and inadequate representation of security-related discourse. Thus, although real-world threats have escalated, the academic exploration of cryptocurrency security seems disjointed and integrated into broader conceptual frameworks.

The findings of the thematic map and the evolution of the cryptocurrency literature indicate a critical research gap, which has motivated the authors to perform a detailed bibliometric analysis focusing on the intersection of *cryptocurrency* and *security*. This analysis provides a focused view of how security is addressed in cryptocurrency research. This study highlights key publication trends, identifies leading contributors, and uncovers gaps in collaboration and topic integration. An interesting aspect of this study is the use of LLMs to standardize affiliation data, significantly enhancing the accuracy of institutional analysis.

## *4.2. Research Questions*

Based on the results of our pilot study, we further delved into the bibliometric analysis of the field “cryptocurrency and security” and developed research questions that can assist us in understanding the existing literature in the area of cryptocurrency and security. This will also help in forecasting the future areas of study for cryptocurrency. The following Research Questions (RQ) serve as a guide for conducting the bibliometric analysis:

1. What are the overall annual publication trends and subject categories in terms of publications in the area of cryptocurrency and security?

2. What are the most prominent research topics and gaps in the field of cryptocurrency and security?

3. Which research papers are highly cited (globally and locally) in cryptocurrency and security research according to the number of citations?

4. How do different sources - conferences versus journals - shape the dissemination, visibility, and long-term influence of research in this field?

5. Which countries and authors have made significant contributions to cryptocurrency and security research?

6. How can LLMs be utilized to improve the accuracy and depth of bibliometric analyses in domains with inconsistent affiliations?

7. Which organizations are the main contributors driving research in the area of cryptocurrency and security?

8. Is security studied as a fundamental component of cryptocurrency research or is it just an afterthought?

### *4.3. Bibliometric Analysis on Dataset D2*

In this section, we present the results of the bibliometric analysis on dataset D2, which consists of the documents on cryptocurrency and security. This section presents answers to research questions framed in the previous section. Table 1summarizes the key characteristics of the dataset D2 as generated by the Biblioshiny web interface. The dataset comprises **2620** documents drawn from **1308** different sources including journals, conference proceedings, and books published in the years 2013 to 2025. It is observed that "cryptocurrency and security" area exhibits a **high annual growth rate (51.8% approx.)**, reflecting its rapid development. Each publication received on average **23.45 citations**, and the dataset includes a total of **84634 references**. Conference papers (1553) make up the majority of the publications, followed by journal articles (965) and review papers (102). The predominance of conference papers highlights rapidly evolving and technology-driven nature of the main theme. The dataset includes 9477 author appearances across all publications, with contributions from roughly 7100 distinct writers. An average of 3.62 co-authors per article indicates the collaborative nature of research in cryptocurrency and security. The tendency towards collaborative work is further supported by the fact that only 211 documents (about 8%) were single-authored. Furthermore, overseas collaborations produced about 24.2% of the articles, demonstrating the field's worldwide reach.

**Table 1**
Details about the dataset D2

| Description | Results |
|---|---|
| Timespan | 2013–2025 (as of 29 May 2025) |
| Sources (Journals, Conferences, Books) | 1,308 |
| Documents | 2,620 |
| Annual growth rate (%) | 51.82 |
| Document average age | 3.62 |
| Average citations per document | 23.45 |
| Average citations per year per document | 3.77 |
| References | 84,634 |
| Single-authored documents | 211 |
| Co-authors per document | 3.62 |
| International co-authorships (%) | 24.24 |

#### *4.3.1. Annual Publication Trends*

Fig. 7 presents the yearwise count of publications included in datasets D1 and D2 - the counts related to cryptocurrency (D1) are represented by a blue line, and the number of publications discussing the security aspect of cryptocurrency (D2) represented by a red line. In particular, this figure shows that cryptographic research has been increasing since 2017, peaking around 2023-2024 with more than 2000 publications per year, thus highlighting the growing interest in cryptocurrency among scientists. A sudden growth in the cryptocurrency research is observed in the year 2019. It may be noted that a major decline is visible in the year 2025, but it can be ignored as only publications till 29 May 2025 are included in the graph.

In contrast, the trajectory of security applications in cryptocurrencies showed promising growth from 2017 to 2019, but plateaued in the following years. Major attacks like the 51 percent attack against the cryptocurrencies' blockchains and routing attack on cryptocurrency (Apostolaki et al., 2017) have been reported frequently, yet research in this field has remained stagnant in the past years. The observed drop in the number of publications in 2024 may not necessarily indicate a drop in research activity. Instead, this can be a reflection of unpublished and in-press articles, and indexing delays. Scopus frequently has significant delays in indexing recently published articles, as Adeosun (2024) points out (Adeosun 2024).

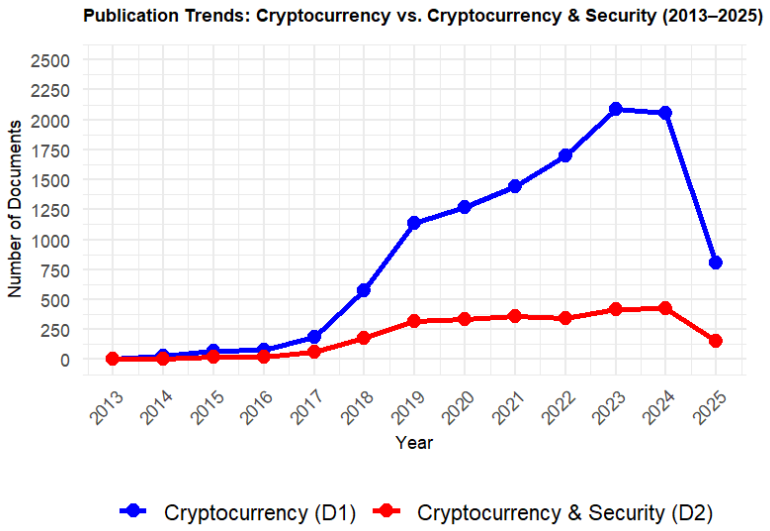


**Fig. 7.** Publication trends for cryptocurrency (D1) and cryptocurrency and security (D2) literature from 2013 to 2025. Note that publications indexed up to 29 May 2025 are included here.

### *4.3.2. Keyword Analysis*

Keywords in a publication are effective indicators of the topics covered, and therefore can be used to identify research trends as well as gaps for the investigated subject area (Ragazou et al., 2022). In preparing the dataset for keyword-based analysis, it was observed that author keywords were missing for 313 publications and index keywords for 568 publications. To ensure comprehensive coverage and minimize data loss, a merged keyword column was created using author keywords where available and falling back to index keywords when author keywords were either missing or invalid (e.g., containing only "NA"). This merged keyword field was then used for treemap visualization using the treemap package in R (Tennekes 2023) and further bibliometric analyses to reflect the true thematic distribution across the dataset.

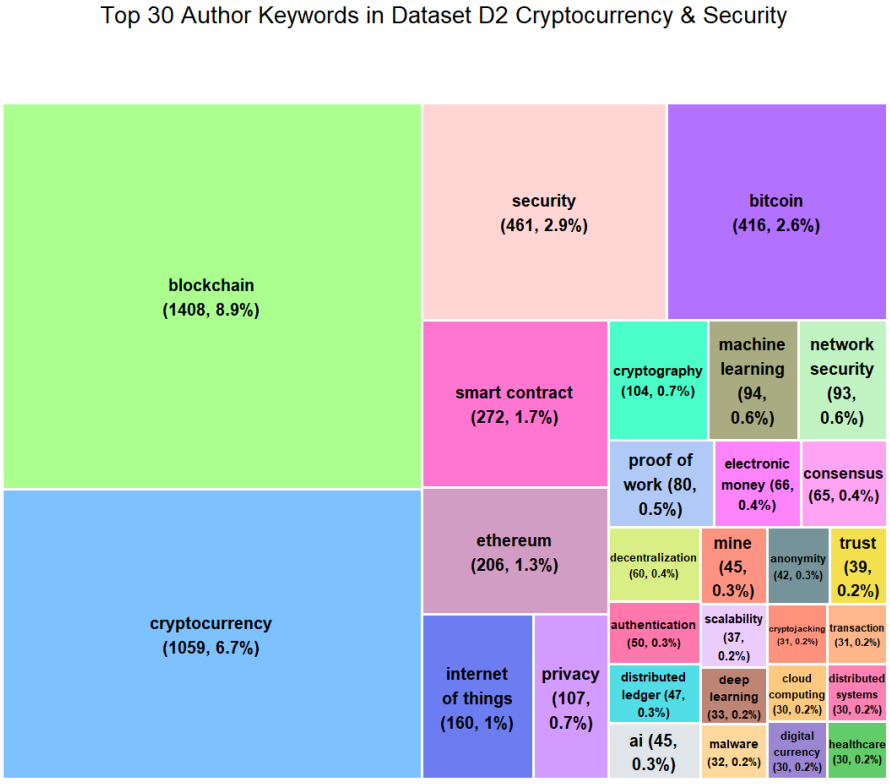


**Fig. 8.** Word Treemap showing the top 30 author keywords in the Cryptocurrency and Security dataset (D2). The relative area of each block represents keyword frequency, with labels showing both count and percentage of total occurrences.

For displaying huge volumes of hierarchically structured data, treemaps are ideal. A quantitative variable is used to size and arrange the space into rectangles. Rectangles that contain other rectangles serve as a visual representation of the levels in the treemap hierarchy. Prior to visualization, a manual keyword normalization procedure was applied to reduce synonym redundancy. Variants such as “crypto-currency”, “crypto wallet”, and “cryptoassets” were combined under a single term, "cryptocurrency," using a custom dictionary in R. A pipeline with dictionary-based mapping and lemmatisation was used to carry out cleanup. The treemap was then manually created using the cleaned keywords, guaranteeing that the visualization appropriately represented actual thematic frequencies rather than fragmented term usage. Fig. 8 presents the Word treemap of the top 20 keywords most commonly used in the publications of the dataset D2. The treemap indicates that *blockchain (8.9%) and cryptocurrency (6.7%)* are the two most frequently cited author keywords. This can be attributed to the fact that all major cryptocurrencies use blockchain technology, with their security guaranteed by a well-secured underlying blockchain. *Security (2.9%)* is a prominent keyword, although considering how important security is to blockchain and cryptocurrency systems, its relative frequency is lower than one might expect. It is quite possible that many studies address the security aspect of cryptocurrency implicitly rather than highlighting it as a primary research keyword. Consequently, specialized security research may be somewhat underrepresented. *Bitcoin (2.6%)* and *Ethereum (1.3%)* are the most prominent electronic cryptocurrencies present in the treemap, indicating that their security concerns have gained significant attention compared to other cryptocurrencies. *Smart contracts (1.7%)* also reflect the rise of programmable decentralized applications. The emergence of keywords like *Internet of Things, machine learning, deep learning*, and *AI* further reflects the multidisciplinary integration of blockchain technology with intelligent systems and emerging technological advances. *Cloud computing* and *distributed systems* indicate broader systems design and deployment contexts. Despite the focus of the dataset on cryptocurrency and security, keywords such as *trust, anonymity, consensus, malware, cryptojacking, privacy, authentication* and *cryptography* appear in significantly lower frequencies. The low frequency of the keyword *healthcare* indicates an emerging interest in blockchain applications for medical domains, with growing relevance in areas like data security and decentralized health finance. This is supported by studies such as (Patel et al., 2024), which highlight the investment and diversification potential of cryptocurrencies focused on healthcare.

### *4.3.3. Most Cited Documents*

The top 10 most globally and locally cited papers are shown in Tables 2 and 3 respectively. While local citations show a publication’s effect inside the currently analyzed dataset (D2 in our case), global citations show how often a publication is cited globally across all sources (WoS, Scopus etc.) (Aria & Cuccurullo 2017).

From Table 2, it can be seen that the most globally cited work belonged to Yli-Huumo J (2016) published in PLOS One and having 1709 citations. The second most globally cited work is that of Li et al. (2020) with 1123 citations. This list is dominated by surveys and systematic reviews (6 out of 10) which indicates that such papers have high academic value. 9 out of 10 papers on this list of highly cited papers appear to have peaked between 2015 and 2020, indicating a period of high academic interest in the area of cryptocurrency and security.

**Table 2**
Top-10 most globally cited papers in dataset D2 (sorted by total number of global citations).

| Year | Authors | Title | Source | Citations |
|---|---|---|---|---|
| 2016 | Yli-Huumo J.; Ko D.; Choi S.; Park S.; Smolander K. | Where is current research on blockchain technology? — A systematic review | PLOS ONE | 1709 |
| 2020 | Li X.; Jiang P.; Chen T.; Luo X.; Wen Q. | A survey on the security of blockchain systems | Future Generation Computer Systems | 1123 |
| 2017 | Kuo T.-T.; Kim H.-E.; Ohno-Machado L. | Blockchain distributed ledger technologies for biomedical and healthcare applications | Journal of the American Medical Informatics Association | 982 |
| 2015 | Garay J.; Kiayias A.; Leonardos N. | The Bitcoin backbone protocol: analysis and applications | EUROCRYPT | 935 |
| 2018 | Fernández-Caramés T.M.; Fraga-Lamas P. | A review on the use of blockchain for the Internet of Things | IEEE Access | 849 |
| 2015 | Bonneau J.; Miller A.; Clark J.; Narayanan A.; Kroll J.A.; Felten E.W. | SoK: research perspectives and challenges for Bitcoin and cryptocurrencies | IEEE Symposium on Security and Privacy | 842 |
| 2017 | Dinh T.T.A.; Wang J.; Chen G.; Liu R.; Ooi B.C.; Tan K.-L. | Blockbench: a framework for analyzing private blockchains | ACM SIGMOD International Conference on Management of Data | 744 |
| 2019 | Salah K.; Rehman M.H.U.; Nizamuddin N.; Al-Fuqaha A. | Blockchain for AI: review and open research challenges | IEEE Access | 716 |
| 2019 | Ali M.S.; Vecchio M.; Pincheira M.; Dolui K.; Antonelli F.; Rehmani M.H. | Applications of blockchains in the Internet of Things: a comprehensive survey | IEEE Internet of Things Journal | 712 |
| 2018 | Conti M.; Sandeep K.E.; Lal C.; Ruj S. | A survey on security and privacy issues of Bitcoin | IEEE Communications Surveys | 712 |

In contrast to most globally cited papers, papers most cited within the dataset D2 (Table 3) tend to emphasize technical foundations, such as consensus protocols, blockchain architecture, and key security issues, thus indicating their central role in shaping research specific to cryptocurrency and security. Although Nakamoto's 2008 research paper on Bitcoin appears as the most locally cited paper in the dataset D2 with 819 citations, it does not appear in the globally cited list. This emphasizes its crucial function in the field of cryptocurrency and security, even if it wasn't retrieved during the initial dataset D2 filtering based on the keywords "cryptocurrency" and "security".

**Table 3**
Top-10 most locally cited papers in dataset D2 (sorted by total number of local citations).

| Year | Authors | Title | Source | Citations |
|---|---|---|---|---|
| 2008 | Nakamoto S. | Bitcoin: a peer-to-peer electronic cash system | Decentralized Business Review | 819 |
| 2017 | Zheng Z.; Xie S. | An overview of blockchain technology: architecture, consensus, and future trends | IEEE Communications Surveys and Tutorials | 218 |
| 2014 | Wood G. | Ethereum: a secure decentralised generalised transaction ledger | Ethereum Project Yellow Paper | 150 |
| 2018 | Eyal I.; Sirer E.G. | Majority is not enough: Bitcoin mining is vulnerable | Communications of the ACM | 134 |
| 2002 | Castro M.; Liskov B. | Practical Byzantine fault tolerance and proactive recovery | ACM Symposium on Operating Systems Principles | 117 |
| 2013 | Decker C.; Wattenhofer R. | Information propagation in the Bitcoin network | IEEE P2P Conference | 116 |
| 2017 | Atzei N.; Bartoletti M. | A survey of attacks on Ethereum smart contracts (SoK) | IEEE European Symposium on Security and Privacy | 112 |
| 2015 | Bonneau J.; Miller A.; Clark J.; Narayanan A.; Kroll J.A.; Felten E.W. | SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies | IEEE Symposium on Security and Privacy | 106 |
| 2016 | Gervais A.; Karame G.O.; Capkun S.; Lenders V. | On the security and performance of proof of work blockchains | ACM SIGSAC Conference on Computer and Communications Security | 90 |
| 2016 | Dorri A.; Kanhere S.S.; Jurdak R. | Blockchain for IoT security and privacy: The case study of a smart home | IEEE International Conference on Pervasive Computing and Communications Workshops | 88 |

An important observation is that just one paper, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies" by (Bonneau et al., 2015), is listed in both the top-10 locally and globally cited lists. This demonstrates its twofold importance: it is very relevant within the specialized field of cryptocurrency and security, and has a wide academic reach globally.

### *4.3.4. Source Analysis*

In this section, we identify the core journals and conferences shaping research in the area of cryptocurrency and security. Source-level analysis is performed on the basis of both the number of articles published and citations received. The most relevant sources are those that contribute most papers in the given field. The most influential sources, identified using average citation counts, reflect the scholarly impact and visibility of a given publication. Figure 9 and Figure 10 show the most relevant and most influential sources respectively in the area of cryptocurrency and security.

It can be seen in Fig. 9 that Lecture Notes in Computer Science (LNCS) has the maximum publications (207) pertaining to "Cryptocurrency and Security" making it the most important repository for research in the studied domain. This is followed by IEEE Access with 78 publications on the same. Fig. 10 indicates IEEE Communications Surveys and Tutorials to be the most influential journal for cryptocurrency and security, with the highest average citations (549.6). It is followed by PLOS ONE (364.8), Future Generation Computer Systems (203.9), ACM Computing Surveys (176.4) and Journal of Network and Computer Applications (142), demonstrating their impact and the importance of the research they publish. An interesting observation is that none of these top 5 sources with highest average citations appear in the top 10 list of sources by publication volume, which indicates their high impact despite low publication volume. The considerable disparity in the kinds of sources that predominate in most relevant sources and most influential sources is one noteworthy finding from the bibliometric investigation. Journals top the list of most influential sources by citations (9 are journals and only one conference proceedings), whereas conference proceedings make up the majority of the most pertinent sources by publication count with only one journal and 9 conference proceedings. This points to a subject where ideas are quickly shared at conferences but that depends on journals for a longer-lasting and wider scholarly influence.

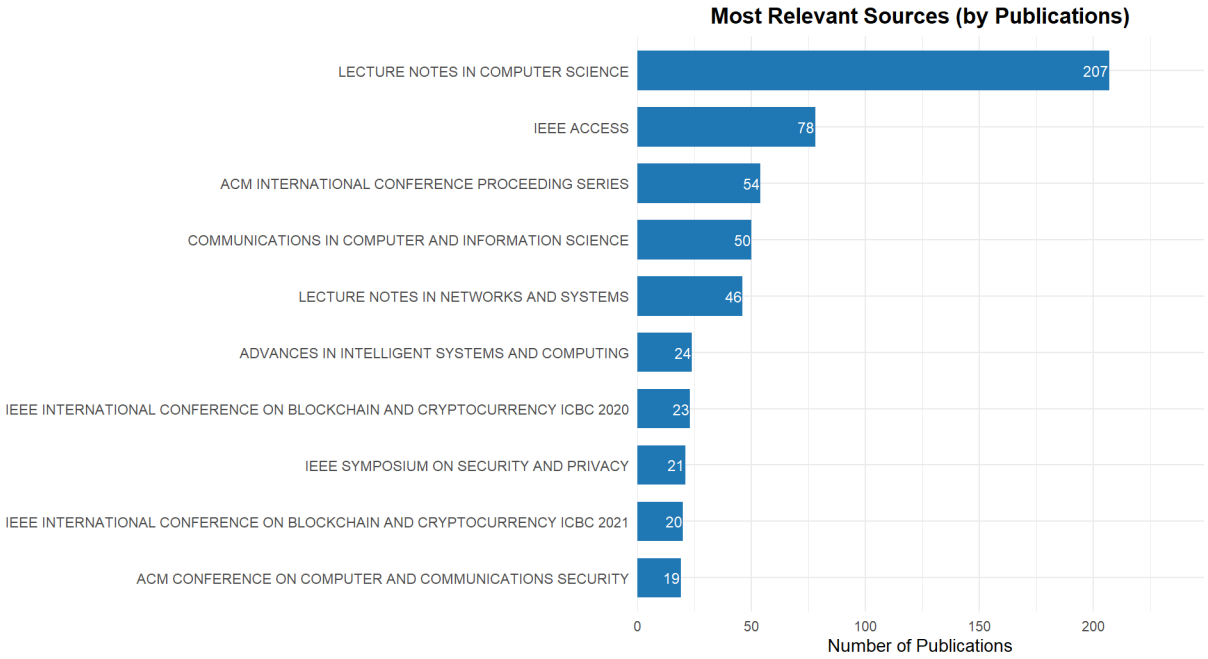


**Fig. 9.** Most relevant sources in cryptocurrency and security (Dataset D2).

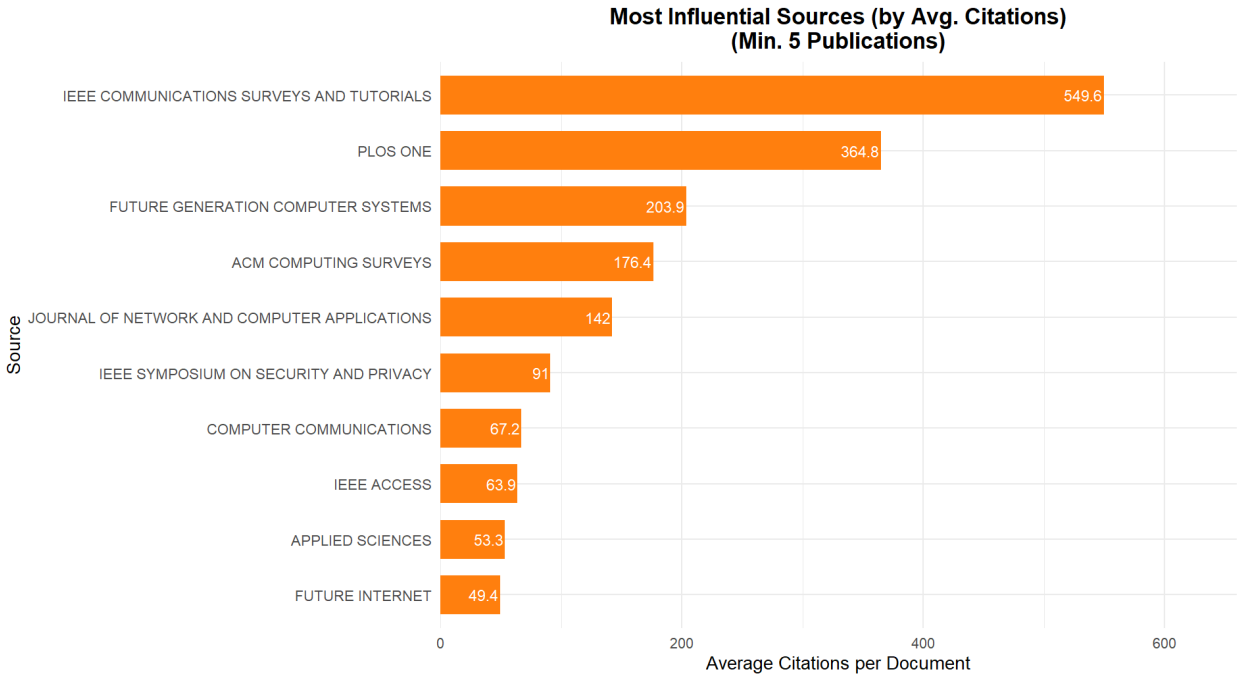


**Fig. 10.** Most influential sources in cryptocurrency and security (Dataset D2).

### *4.3.5. Geographical Trends*

Gaining insight into the work done across the world on security applications in cryptocurrencies becomes possible by tracking the number of publications originating from each nation, by considering the number of citations for publications originating from a country or by considering the collaborations across nations for publications on the subject.

The *country scientific production* is calculated, considering the geographic locations associated with the authors of each such publication. For each work, a point is allocated to each nation of the relevant affiliated authors (Zennaro et al., 2021). The number of publications originating from a country directly relate to the color intensity. Fig. 11 created via Biblioshiny web interface, captures the geographical distribution of the research publications on cryptocurrency and security across the world. The intensity of blue colour on the map is indicative of the number of publications originating from that area. Dark blue areas on the map indicate areas with a large number of publications on the subject, and white/ light blue areas indicate otherwise. It is evident from the figure that research on this subject is gaining traction in the Asian continent. India registered the highest number of papers (1952), followed by China (1452) and USA (1224).

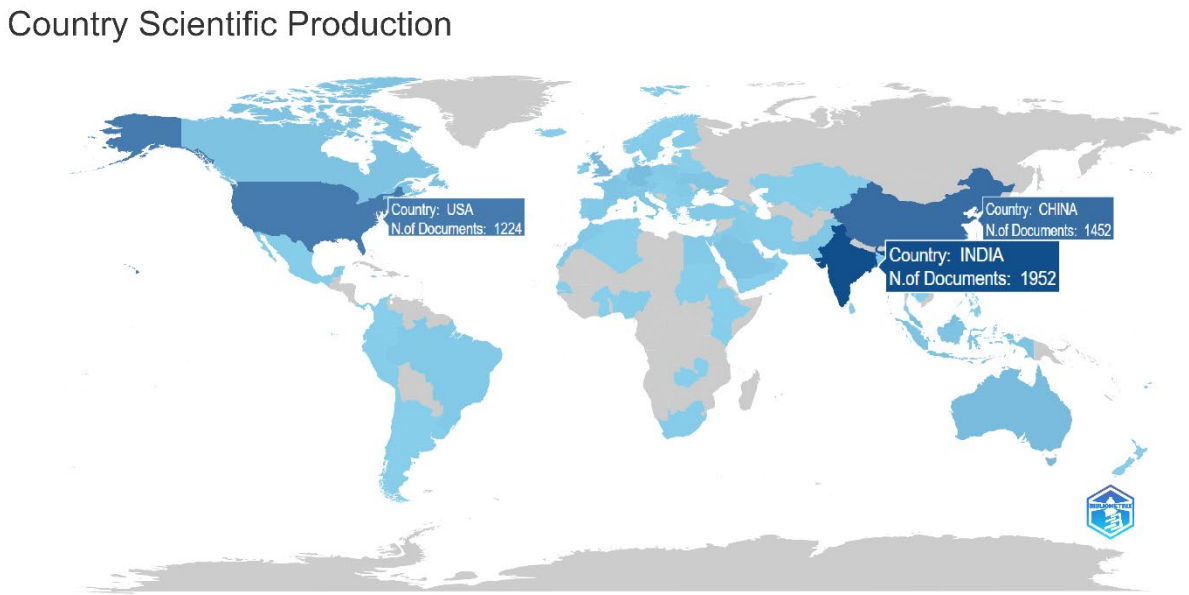


**Fig. 11.** Geographical distribution of the publications on cryptocurrency and security (Dataset D2). The color intensity is directly proportional to the number of publications.

Fig. 12 created via VOSviewer, presents the citation and collaboration network across various countries of the world, where each paper is assigned to the geographical location of the author.

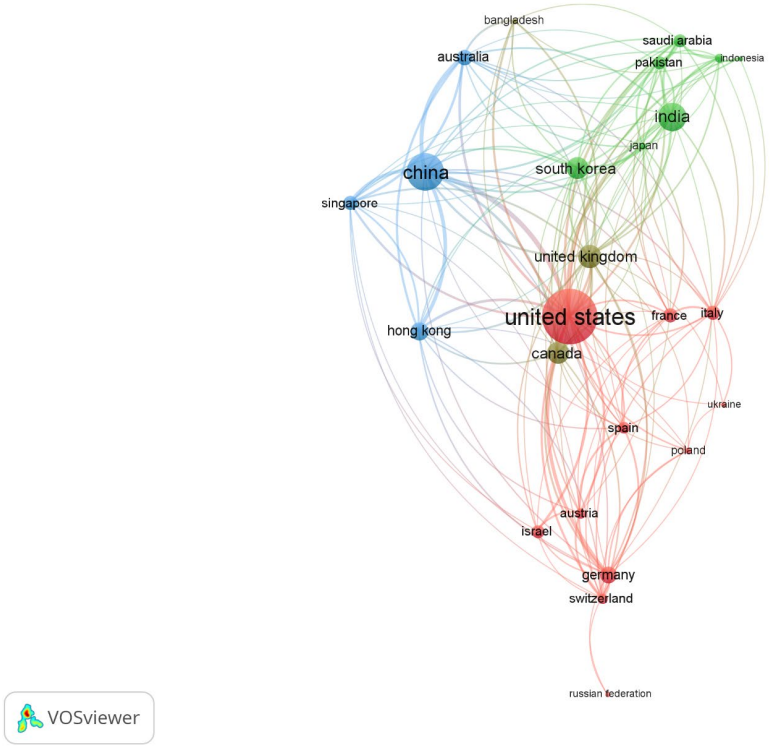


**Fig. 12.** Top cited countries for documents discovered in the field of cryptocurrency and security (Dataset D2).

The number of total citations linked to a country is reflected in the size of the node. Countries with more research influence are indicated by larger nodes. The strength of co-authorship between countries is indicated by the link thickness. More frequent collaborations are indicated by thicker links. It is evident from the size of nodes in the figure that the United States leads in producing the most influential publications in the field of cryptocurrency & security, having the highest number of citations, followed by China and India. The thick link between the USA and China is indicative of a significant amount of joint research in cryptocurrencies and security between the two countries, despite political and regulatory concerns. Interestingly, China is involved in four of the strongest co-authorship relationships despite the fact that China does not have the

most papers or citations in the subject. Communities of countries that collaborate more frequently are shown by clusters (denoted by color). The blue cluster comprising of China, Singapore, Hong Kong, and Australia represents a strategic Asia-Pacific research partnership. Despite their differences in size and productivity, these countries share strong collaborative ties, especially with China serving as a key hub. The red cluster in the co-authorship network map includes USA, France, Germany, Switzerland, Spain, Italy, Poland, Austria, Ukraine, and Israel. This cluster forms a a strong transatlantic and European research network with the USA being the central connector. The yellow cluster creates a network of cross-continental collaboration between the United Kingdom, Bangladesh, and Canada. The concentration of research conducted in this field suggests that cryptocurrency and security research has been primarily carried out in developed countries and a few developing countries in European and Asian regions. India has made significant strides in the field of cryptocurrency and security, boasting the highest number of documents on the subject. However, it still lags behind the USA and China in terms of citations received for its research.

### *4.3.6. Academic Leaders*

In this section, we present an analysis of the academic organizations leading the research output in the area of cryptocurrency and security. To perform this analysis, the affiliations of the authors need to be considered. But it requires handling a well-known problem regarding the inconsistency in the name of institute/ organization, as the name of an institute may appear in different formats (Mazov and Gureyev 2018). To address this issue, we harmonized and standardized the organization names using a locally run *LLaMa 3:8B* (LLaMA Team 2024) (Meta AI 2024), an open source large language model released by Meta AI, which is instruction-fine-tuned with 8 billion parameters that can support a broad range of use cases. We selected the LLaMa 3:8B model because it offers the best performance and resource efficiency balance. The model was run through the *Ollama* framework (Ollama 2023). Ollama framework was created to make it easier to deploy and run LLMs for a variety of language analytics applications. Specifically, we identified and extracted standardised parent institution names from raw affiliation strings. The model was instructed via the following attributed prompt:

*Extract and harmonize the full name of the main parent university or research institute from the academic affiliation below. Do not guess or assume the institution name. Do not modify or substitute acronyms. Do not include city, department, or country. Return ONLY the exact institute name as given, in full and in uppercase. No extra text, explanation, or line breaks at all.*

The prompt ensured that only the core institution name in uppercase be produced as the output. A one-to-one mapping table was then created using the harmonized affiliations that were produced, followed by manual validation to ensure high accuracy. This allowed for precise institutional-level aggregation of document counts and co-authorship link strengths. In contrast, the unharmonized and unrefined dataset of affilations significantly misrepresented organizational contributions due to inconsistent naming.

**Table 4**
**Top Universities by Document Count and Link Strength**

| University | Documents | Link Strength |
|---|---|---|
| CHINESE ACADEMY OF SCIENCES | 31 | 66 |
| UNIVERSITY OF TEXAS | 30 | 59 |
| CHITKARA UNIVERSITY | 27 | 35 |
| AMITY UNIVERSITY | 26 | 21 |
| GRAPHIC ERA UNIVERSITY | 25 | 87 |
| UNIVERSITY COLLEGE LONDON | 23 | 38 |
| UNIVERSITY OF CALIFORNIA | 23 | 45 |
| SHANGHAI JIAO TONG UNIVERSITY | 22 | 40 |
| SRM INSTITUTE OF SCIENCE & TECHNOLOGY | 22 | 20 |
| WUHAN UNIVERSITY | 21 | 66 |
| MONASH UNIVERSITY | 21 | 51 |
| UNIVERSITY OF CHINESE ACADEMY OF SCIENCES | 20 | 42 |

Table 4 displays the list of top universities with a publication output of more than 20. **The link strength indicates how frequently two organizations have collaborated as co-authors across the dataset.** Eight out of the top 12 most prominent institutions are situated in the Asian continent, particularly in China and India, while the other four hail from UK, USA and Australia. In terms of publishing volume, the Chinese Academy of Sciences leads with 31 papers, closely followed by Chitkara University (27 papers) and the University of Texas (30 papers). Despite having comparatively fewer documents (25), Graphic Era University stands out as having the strongest overall link strength (87), suggesting a highly collaborative publication approach with regular inter-institutional co-authorship. Strong international research engagement is demonstrated by institutions like the University of California, Monash University, and University College London, which combine a significant output with a noticeable level of collaboration. On the other hand, organisations such as SRM Institute of

Science & Technology and Amity University have moderate levels of collaboration, indicating the possibility of growing research alliances.

### *4.3.7. Co-Citation Analysis*

Co-citation analysis is the most effective method for examining the frequency with which two or more papers or authors are jointly cited in other works, thus revealing potential connections and associations between them. To perform this analysis, we selected authors whose publications on the subject had accrued a minimum of 300 citations. The selection criterion ensured the inclusion of influential and well-recognized research. As a result, only 26 authors matching the citation threshold were selected out of a total of 81029 authors. Fig. 13 presents the co-citation network for the 26 selected authors created via VOSviewer. Here, the size of the circle reflects the number of citations of the author and the thickness of link between two authors indicates the number of times two authors are cited together.

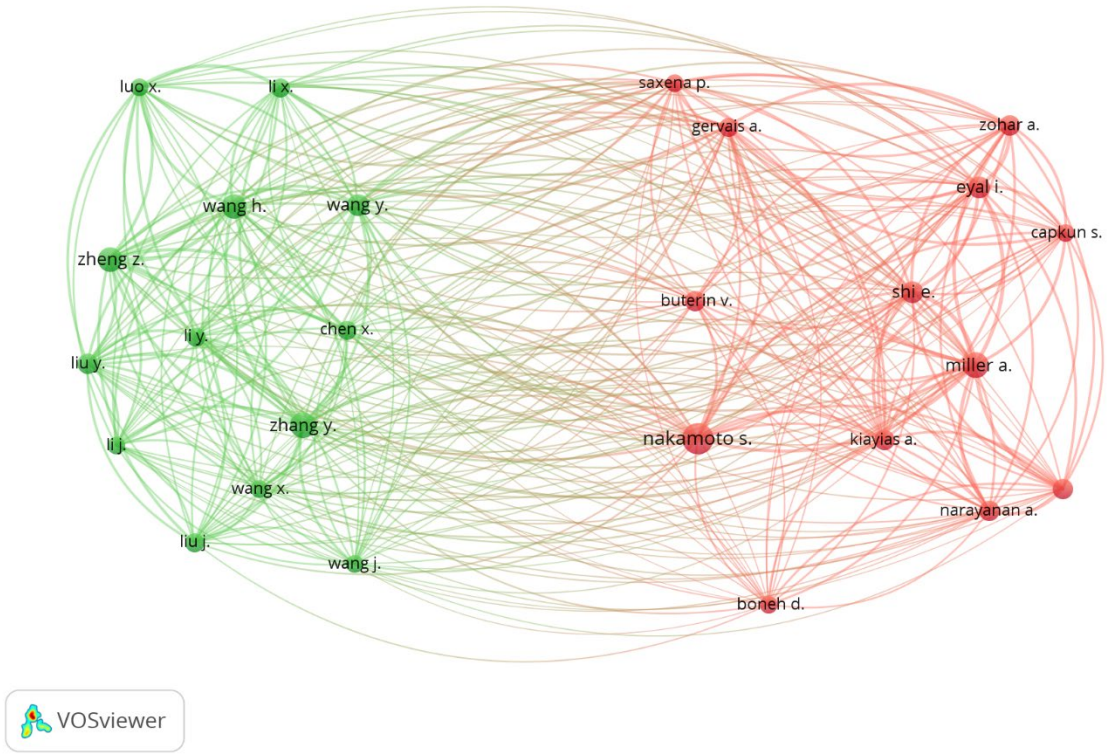


**Fig. 13.** Visualization map showing co-citation analysis of the top authors (having more than 300 citations) in the field of cryptocurrency and security (Dataset D2).

Nakamoto S. stands out as the most influential author in cryptocurrency & security, having been cited 926 times followed closely by Millar A. with 638 citations. Miller A. though has the highest total link strength that means his work is most frequently co-cited with others. These authors have significant influence in the cryptocurrency & security domain and enjoy widespread citation. The two clusters (red and green) observed in the figure indicates that the authors in each cluster are co-cited together more often. The red cluster is centered by Nakamoto S. (author of the foundational bitcoin paper (Nakamoto 2008)), Buterin V. (author of the ethereum foundational paper (Buterin 2014)) and Miller A., thereby indicating that the citations in the research papers on cryptocurrency and security is still dominated by the authors who worked on the foundational cryptocurrency research.

### *4.3.8. Co-Word Analysis*

In this section, we perform co-word analysis of terms present in the title or abstract of the publications on given subject to identify the pairs of terms that often appear together in a publication. This analysis goes beyond the author keywords to uncover ideas and fresh trends in the area of cryptocurrency and security. A co-word analysis of 44 terms, each with frequency more than 200, is presented in Fig. 14, created by using VOSviewer. The size of each circle represents the frequency with which the corresponding terms have appeared in the abstract or title section. The links indicate the number of times two terms appear together and the cluster (indicated by red/green colors) represent groups of keywords that tend to co-occur.

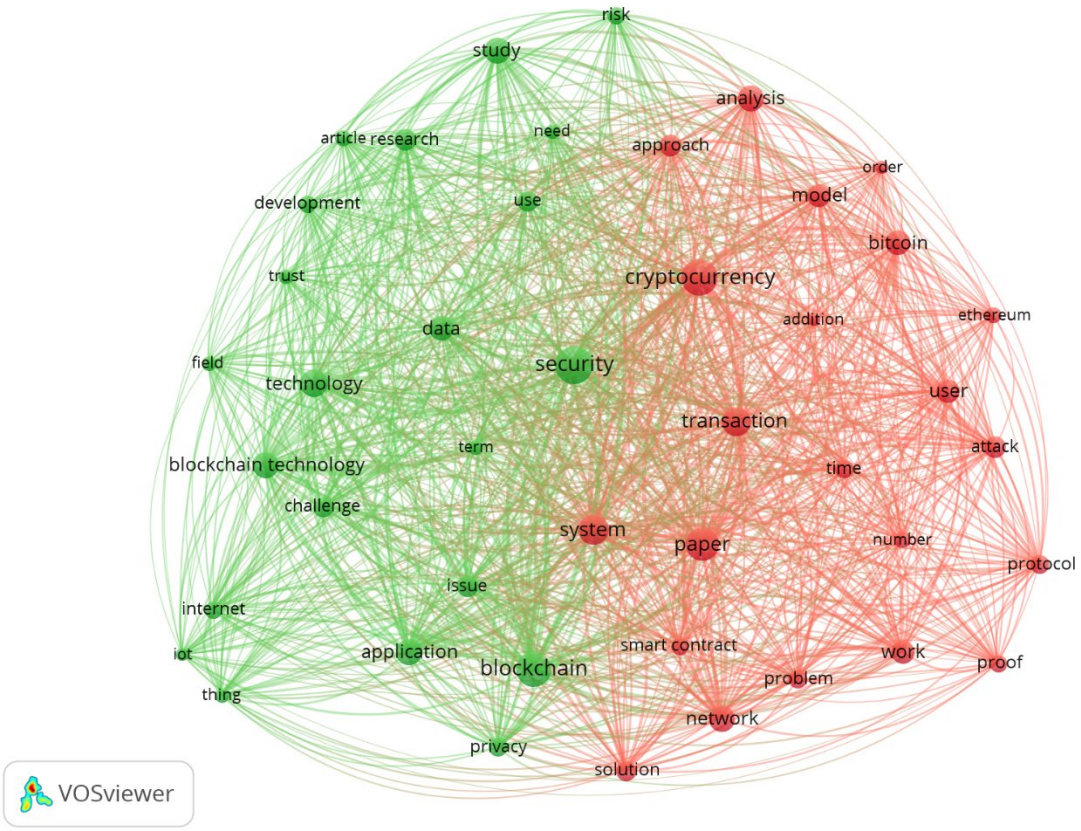


**Fig. 14.** Co-word map of the most frequent terms discovered based on the article title or abstract, in the field of cryptocurrency and security (Dataset D2).

Due to the extraction of dataset D2 based on the keywords - *Cryptocurrency* and *Security*, these words are also found to be the most frequent terms in Figure 14. The red cluster is dominated by the terms like - *bitcoin*, *ethereum*, *transaction*, *protocol*, and *model*, thereby indicating a cluster that focuses on the functioning and modeling of cryptocurrencies. On the other hand, the green cluster is dominated by terms like *data*, *technology*, *risk*, *trust*, and *IoT* demonstrating that this cluster related to security challenges, risk management and technological development for secure systems. The conceptual clusters indicate the need of more fundamental research that approaches security as a fundamental component of cryptocurrency systems rather than as an afterthought.

## 5. Conclusion

This study begins with the bibliometric analysis of cryptocurrency-related research, which revealed a critical knowledge gap of focused work on cryptocurrency and security despite their growing significance. This observation motivated a more targeted bibliometric analysis of literature at the intersection of cryptocurrency and security, extensively covering publication trends, keyword analysis, co-word analysis, geographical distribution, and author influence along with co-citation analysis. With only 8% of publications being single-authored and over 24% including international collaborations, the analysis shows a clear trend towards collaborative research. Review papers dominate global citations, while locally cited works emphasize on the technical aspects. LNCS leads in publication volume, while high-impact journals like IEEE Communications Surveys and Tutorials show strong influence despite fewer publications. The findings underscore a marked increase in global research output, with the United States emerging as leading contributor in terms of publication volume and citation impact. The co-citation analysis across the world highlights robust international collaborations, particularly between the United States and China, despite geopolitical complexities. India has made significant strides in the field of cryptocurrency and security, boasting the highest number of documents on the subject. Most prominent institutions with a large volume of publications are situated in the Asian continent, particularly in China and India. Keyword analysis indicates focus on topics like *blockchain*, *cryptocurrency* and *security* and security concerns mostly addressed for *Bitcoin* and *Ethereum*. The identification of highly cited publications and authors offers valuable insights into the intellectual structure of the field. Conferences promote quick dissemination; journals ensure lasting impact. A co-word analysis of publications reveals two clusters, one focuses on the functioning and modeling of cryptocurrencies and the other related to security challenges, risk management and technological development for secure systems. Co-word citation of terms in abstract or title resulted in creation of two conceptual clusters, one focusing on crytocurrency and the other on security, thereby highlighting the need of more

comprehensive and multidisciplinary research that approaches security as a fundamental component of cryptocurrency systems rather than as an afterthought. An interesting aspect of this study is the use of LLMs to standardize affiliation data, significantly enhancing the identification of academic leaders. Overall, this bibliometric analysis not only delves into research in cryptocurrency and security but also provides a solid reference for researchers exploring the rapidly evolving area of security issues in cryptocurrency.

**Acknowledgement**

This research follows from the project work done as part of the Annual Research Programme (ARP) 2023 organized by the Centre for Research, Maitreyi College, University of Delhi.

**Data Availability**

The data that support the findings of this study are available in the Scopus database (www.scopus.com) and Web of Science (WoS) database (www.webofscience.com).

**References**

Adeosun, S. (2024). Scopus indexing delays of articles published in major pharmacy practice journals. *Innovations in Pharmacy, 15*(4), Article 6322. https://doi.org/10.24926/iip.v15i4.6322

Aghaei Chadegani, A., Salehi, H., Yunus, M., Farhadi, H., Fooladi, M., Farhadi, M., & Ale Ebrahim, N. (2013). A comparison between two main academic literature collections: Web of Science and Scopus databases. *Asian Social Science, 9*(5), 18–26. https://doi.org/10.5539/ass.v9n5p18

Al-Ali, R., Mekimah, S., Zighed, R., & Bourahla, M. (2025). Evolution and gaps in data mining research: Identifying the bibliometric landscape of data mining in management. *Decision Science Letters, 14*(2), 435–448. https://doi.org/10.5267/j.dsl.2024.12.011

Al-Raggad, M. (2025). Deepfake crimes in the age of AI: A bibliometric study of emerging risks and research trends. *International Journal of Data and Network Science, 10*(1), 15–26. https://doi.org/10.5267/j.ijdns.2025.10.016

Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing attacks on cryptocurrencies. *2017 IEEE Symposium on Security and Privacy (SP)*, 375–392. https://doi.org/10.1109/SP.2017.29

Aria, M., & Cuccurullo, C. (2017). Bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics, 11*(4), 959–975. https://doi.org/10.1016/j.joi.2017.08.007

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015, May). SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies. *2015 IEEE Symposium on Security and Privacy (SP)*, 104–121. https://doi.org/10.1109/SP.2015.14

Buterin, V. (2014). *A next-generation smart contract and decentralized application platform* [White paper]. Ethereum. https://ethereum.org/en/whitepaper/

Chaum, D. (1983). Blind signatures for untraceable payments. In D. Chaum, R. L. Rivest, & A. T. Sherman (Eds.), *Advances in cryptology: Proceedings of Crypto 82* (pp. 199–203). Plenum Press.

Chaum, D., Fiat, A., & Naor, M. (1990). Untraceable electronic cash. In S. Goldwasser (Ed.), *Advances in Cryptology—CRYPTO' 88* (pp. 319–327). Springer.

Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of Bitcoin. *IEEE Communications Surveys & Tutorials, 20*(4), 3416–3452. https://doi.org/10.1109/COMST.2018.2842460

De Bellis, N. (2009). *Bibliometrics and citation analysis: From the Science Citation Index to cybermetrics*. Scarecrow Press.

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research, 133*, 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

Esfahani, H., Tavasoli, K., & Jabbarzadeh, A. (2019). Big data and social media: A scientometrics analysis. *International Journal of Data and Network Science, 3*(3), 145–164.

Guo, Y.-M., Huang, Z.-L., Guo, J., Li, H., Guo, X.-R., & Nkeli, M. J. (2021). A bibliometric analysis and visualization of blockchain. *Future Generation Computer Systems, 116*, 316–332. https://doi.org/10.1016/j.future.2020.10.023

He, Q. (1999). Knowledge discovery through co-word analysis. *Library Trends, 48*(1), 133–159.

Isaac, C. L. (2022). *Digital money: The law of crypto currency and cryptography in Uganda*. Jescho Publishing House.

Islam, M. R., Rahman, M., Mahmud, M., Rahman, M., Mohamad, M. H. S., & Embong, A. H. (2021, August). A systematic literature review on blockchain-based access control for IoT systems. *2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC)*, 227–232. https://doi.org/10.1109/ICSGRC53186.2021.9515276

Lim, I.-K., Kim, Y.-H., Lee, J.-G., Lee, J.-P., Nam-Gung, H., & Lee, J.-K. (2014). The analysis and countermeasures on security breach of Bitcoin. In *Computational science and its applications--ICCSA 2014* (pp. 720–732). Springer International Publishing.

LLaMA Team. (2024). *The Llama 3 herd of models*. arXiv. https://arxiv.org/abs/2407.21783

Mazov, N. A., & Gureyev, V. N. (2018, August). Modern challenges in bibliographic metadata identification. *2018 3rd Russian-Pacific Conference on Computer Technology and Applications (RPC)*, 1–4. https://doi.org/10.1109/RPC.2018.8482205

Melcer, E., Nguyen, T.-H. D., Chen, Z., Canossa, A., Seif El-Nasr, M., & Isbister, K. (2015). Games research today: Analyzing the academic landscape 2000-2014. *Proceedings of the 10th International Conference on the Foundations of Digital Games (FDG 2015)*.

Meta AI. (2024). *Meta Llama 3*. https://llama.meta.com/models/llama-3/

Mongeon, P., & Paul-Hus, A. (2016). The journal coverage of Web of Science and Scopus: A comparative analysis. *Scientometrics, 106*(1), 213–228. https://doi.org/10.1007/s11192-015-1765-5

Muñoz-Leiva, F., Viedma-del-Jesús, M. I., Sánchez-Fernández, J., & López-Herrera, A. G. (2012). An application of co-word analysis and bibliometric maps for detecting the most highlighting themes in the consumer behaviour research from a longitudinal perspective. *Quality & Quantity, 46*, 1077–1095. https://doi.org/10.1007/s11135-011-9568-0

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

Nasir, A., Shaukat, K., Khan, K. I., Hameed, I. A., Alam, T. M., & Luo, S. (2021). What is core and what future holds for blockchain technologies and cryptocurrencies: A bibliometric analysis. *IEEE Access, 9*, 989–1004. https://doi.org/10.1109/ACCESS.2020.3046931

Navamani, T. M. (2023). A review on cryptocurrencies security. *Journal of Applied Security Research, 18*(1), 49–69. https://doi.org/10.1080/19361610.2021.1933322

Ollama. (2023). *Ollama: Run open-source large language models locally*. https://ollama.com/

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

Pandya, S., Mittapalli, M., Gulla, S. V. T., & Landau, O. (2019). Cryptocurrency: Adoption efforts and security challenges in different countries. *Holistica – Journal of Business and Public Administration, 10*(2), 167–186. https://doi.org/10.2478/hjbpa-2019-0024

Patel, R., Gubareva, M., Chishti, M. Z., & Teplova, T. (2024). Connectedness between healthcare cryptocurrencies and major asset classes: Implications for hedging and investments strategies. *International Review of Financial Analysis, 93*, 103181. https://doi.org/10.1016/j.irfa.2024.103181

Pritchard, A. (1969). Statistical bibliography or bibliometrics. *Journal of Documentation, 25*(4), 348–349.

Ragazou, K., Passas, I., & Sklavos, G. (2022). Investigating the strategic role of digital transformation path of SMEs in the era of COVID-19: A bibliometric analysis using R. *Sustainability, 14*(18), 11295. https://doi.org/10.3390/su141811295

Ramos-Rodríguez, A.-R., & Ruíz-Navarro, J. (2004). Changes in the intellectual structure of strategic management research: A bibliometric study of the *Strategic Management Journal*, 1980–2000. *Strategic Management Journal, 25*(10), 981–1004. https://doi.org/10.1002/smj.397

Sarkar, S., Roy, H., & Mazumder, S. (2020). Citation analysis of scholarly publications on indigenous knowledge. *Library Philosophy and Practice (e-Journal)*, 4851. https://digitalcommons.unl.edu/libphilprac/4851

Scopus. (2025). *Scopus database*. Elsevier.

Tennekes, M. (2023). *Treemap: Treemap visualization* (R package version 2.4-4) [Computer software]. https://cran.r-project.org/package=treemap

Van Eck, N. J., & Waltman, L. (2014). Visualizing bibliometric networks. In Y. Ding, R. Rousseau, & D. Wolfram (Eds.), *Measuring scholarly impact: Methods and practice* (pp. 285–320). Springer International Publishing. https://doi.org/10.1007/978-3-319-10377-8_13

Van Raan, A. F. J. (2005). For your citations only? Hot topics in bibliometric analysis. *Measurement: Interdisciplinary Research and Perspectives, 3*(1), 50–62. https://doi.org/10.1207/s15366359mea0301_7

Web of Science. (2025). *Web of Science database*. Clarivate Analytics.

Yuan, K., Zhu, G., & Zhu, X. (2022). Blockchain security research progress and hotspots. *IAENG International Journal of Computer Science, 49*(2), 206–213.

Zennaro, F., Furlan, E., Simeoni, C., Brigolin, D., & Rubino, F. (2021). Exploring machine learning potential for climate change risk assessment. *Earth-Science Reviews, 220*, 103752. https://doi.org/10.1016/j.earscirev.2021.103752

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services, 14*(4), 352–375. https://doi.org/10.1504/IJWGS.2018.095647

© 2026 by the authors; licensee Growing Science, Canada. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (http://creativecommons.org/licenses/by/4.0/).