applied sciences

MDPI

Review

A Systematic Literature Review of Current Trends in Electronic Voting System Protection Using Modern Cryptography

Tolegen Aidynov [1], Nikolaj Goranin [2], Dina Satybaldina [1] and Assel Nurusheva [1,*]

[1] Department of Information Security, Faculty of Information Technologies, L.N. Gumilyov Eurasian National University, Astana KZ-010000, Kazakhstan; 951005351309@enu.kz (T.A.); satybaldina_dzh@enu.kz (D.S.)
[2] Department of Information Systems, Faculty of Fundamental Sciences, Vilnius Gediminas Technical University, LT-08412 Vilnius, Lithuania; nikolaj.goranin@vilniustech.lt
* Correspondence: asselnurusheva7@gmail.com

Abstract: Electronic voting, based on cryptographic protocols and blockchain technology, represents an advanced method for ensuring the security, transparency, and reliability of electoral processes. The scientific research presented in this article is devoted to the analysis of trends and advanced technologies in the field of electronic voting. The authors propose a systematic mapping of this area using bibliometric analysis. The research is based on the analysis of scientific articles extracted from the Web of Science and Scopus databases. Bibliometric analysis tools are used to automatically identify key topics and trends in the literature. The results of the study reveal the key directions of the development of electronic voting, including the integration of cryptographic protocols and blockchain technology. Specific aspects include improving privacy through the use of modern cryptographic protocols, creating an immutable register of votes using blockchain technology, ensuring trust through open-source code, and increasing resilience to cyber-attacks. These areas reflect the desire to develop efficient, transparent, and secure electronic voting systems. Based on the identified trends, recommendations are proposed for further research aimed at improving electronic electoral systems and their adaptation to the modern requirements of security and transparency in electoral processes.

Keywords: bibliometric analysis; electronic voting; cryptographic protocols; blockchain; systematic mapping

check for updates

Citation: Aidynov, T.; Goranin, N.; Satybaldina, D.; Nurusheva, A. A Systematic Literature Review of Current Trends in Electronic Voting System Protection Using Modern Cryptography. *Appl. Sci.* **2024**, *14*, 2742. https://doi.org/10.3390/app14072742

Academic Editor: Andrea Prati

Received: 20 February 2024
Revised: 14 March 2024
Accepted: 21 March 2024
Published: 25 March 2024

1. Introduction

In the modern information society, electronic voting is becoming a key element of democratic processes, providing citizens with an effective and convenient mechanism for participating in elections. Electronic voting (EV), based on cryptographic protocols and blockchain technology, is an innovative direction in the field of information technology, which brings significant changes to the conduct of elections and referendums [1]. However, despite numerous advantages, such as reducing the time for counting votes, improving accessibility, and improving the efficiency of electoral processes, electronic voting also faces serious challenges related to the security and confidentiality of voting.

Every year, innovative methods of electronic voting are being developed, providing some protection against fraud and guaranteeing the reliability of the process itself. These technologies have given rise to new methods of electronic voting [2], which, despite their importance, also pose serious challenges to the democratic system. Electronic voting significantly increases the reliability of elections compared to traditional methods, ensuring the efficiency and integrity of the process [3]. Due to its flexibility, ease of use, and low cost compared to traditional elections, electronic voting is widely used for making various decisions [4]. Nevertheless, the existing methods of electronic voting involve the risk of excessive centralization and the possibility of manipulation, which creates restrictions in ensuring the fundamental fairness, confidentiality, secrecy, anonymity, and transparency of voting.

To address these challenges and explore the potential of cryptographic protocols and blockchain technology in enhancing electronic voting systems, this study is structured around several key research questions.

This research focuses on conducting a systematic mapping study (SMS) to develop a structure for exploring electronic voting based on cryptographic protocols and blockchain technology. The aim is to capture the fundamental concepts in this field. This leads to the main research question (MRQ): How does the use of cryptographic protocols and blockchain technology contribute to electronic voting? From the MRQ, the following research questions (RQs) are formulated:

RQ-1: What are the results of an analysis of electronic voting, cryptographic protocols, and blockchain technology research history?

RQ-2: What aspects are being considered for the study of electronic voting based on cryptographic protocols and blockchain technology?

RQ-3: What is the main direction of the future development of the topic under study?

RQ-4: What is the experience and level of progress of various countries in the deployment of electronic voting systems using cryptographic protocols and blockchain technology?

To ensure the reliability, transparency, and privacy of electronic voting and prevent possible attacks on electoral systems, researchers and developers are increasingly turning to cryptographic protocols and blockchain technology. Cryptographic methods make it possible to ensure the security of data transmission and authentication of votes, and the blockchain, in turn, provides a decentralized and reliable system for storing electoral data.

The present study is aimed at a systematic study of methods and algorithms for organizing electronic voting using cryptographic protocols and blockchain technology. The authors seek to deepen the understanding of security and privacy issues in the context of electronic voting based on advanced cryptographic methods and principles of blockchain technology.

In the course of our research, we will pay attention to the existing risks in the field of electronic voting, analyze modern cryptographic protocols used to ensure the security of electoral processes, and consider the possibilities of integrating blockchain technology to create stable and transparent voting systems.

The main goal is to contribute to the development of effective and safe methods of electronic voting, increasing the level of citizens' confidence in this method of participation in democratic processes.

Within the framework of this study, a comprehensive systematic mapping study (SMS) is conducted, aimed at analyzing existing methods and technologies in the field of electronic voting. Bibliometric analysis is used to identify key trends and directions of development in this field.

The results of this study allow us to conclude that electronic voting systems based on cryptographic protocols and blockchain contribute to the stability and reliability of electoral processes. Such systems have the potential for widespread implementation, which contributes to maintaining democratic principles and increasing voter confidence in elections in various countries. In addition, this study highlights possible areas for further research aimed at improving the technological aspects and social acceptability of electronic voting systems.

The article follows a structured format, beginning with Section 2, which outlines the research scope and methods. The research scope and methods section covers research design, including conducting the search, research selection, and quality assessment. The tools used, the data extraction process, the method for result analysis, and the reliability assessment are detailed. Section 3 presents the results, delving into the study of chronological distribution, frequency of keyword usage, identification of the most common and moderately frequent keywords, and exploration of countries participating in the study. The article concludes with a discussion and conclusions.

2. Research Scope and Methods

Literature reviews performed before have provided a lot of valuable information, highlighting the possibilities for future research on electronic voting, but there is still a need for a holistic and systematic review of the literature on electronic voting based on cryptographic protocols and blockchain technology from the point of view of information security since previous reviews mainly concentrated on broader aspects, such as usability and implementation challenges. This gap underscores the necessity for a focused exploration of the specific intersection of cryptographic protocols, blockchain technology, and information security in the context of electronic voting. Additionally, existing reviews have often been time-sensitive and may not encompass the latest advancements and emerging threats in the rapidly evolving landscape of secure e-voting systems. Therefore, this comprehensive review seeks to bridge these gaps, providing an up-to-date and in-depth analysis of the current state of research on electronic voting, with a keen focus on the robustness and resilience offered by cryptographic protocols and blockchain technology. The motivation behind this endeavor lies in equipping researchers and practitioners with a thorough understanding of the evolving security landscape, ultimately contributing to the advancement of secure, transparent, and trustworthy electronic voting systems in the future.

In [5,6], reviews of the literature on blockchain are given and cover several topics of information security related to blockchain, based on a systematic review of the literature.

In [7], the authors conducted a systematic review of the blockchain literature from the point of view of information systems. A systematic review was carried out by a method based on the proposals of Webster and Watson [8] and the practices of Steininger [9]. The authors conducted a literature search using the principles of a consistent approach [10,11], which ensured consistency, reproducibility, and transparency of the research results. This review, while comprehensive in its examination of the blockchain literature from the perspective of information systems, may not be directly suitable for our article due to the specific focus on information systems rather than electronic voting. The relevance of the review depends on the alignment of its research questions and objectives with our specific focus on the application of blockchain technology in electronic voting systems. Therefore, the article may not provide the targeted insights needed for our research agenda in the context of electronic voting security.

The authors in [12] conducted a comprehensive evaluation of several articles on blockchain technology in information systems, providing a complete list of applications systematized on problems related to blockchain technology. To identify and analyze the existing literature and conduct methodological research on these topics, the authors used digital libraries such as IEEE Xplore, Scopus, ScienceDirect, SpringerLink, and ACM Digital Library. It is crucial to note certain limitations in their research. These limitations may include potential publication bias, as the selection of articles from specific digital libraries could inadvertently exclude relevant research published elsewhere. Additionally, the dynamic nature of blockchain technology may lead to the omission of recent advancements or emerging challenges.

Given our specific focus on blockchain technology in the context of electronic voting, it is essential to consider whether the reviewed articles directly address the unique challenges and applications within the realm of secure and transparent voting systems. Further insights into the methodology's rigor, such as criteria for article inclusion and potential subjective biases in the evaluation process, would enhance the transparency and reliability of their findings in the context of our research agenda on blockchain technologies in voting systems. Addressing these limitations would provide a more nuanced understanding of the scope and applicability of blockchain technology in electronic voting.

In their review of electronic voting, the authors in [13] present a description and comparison of various electronic voting systems based on blockchain technology. The authors offer a review of electronic voting systems based on blockchain technology, presenting a description and comparison; however, it is crucial to seek more detailed information on the specific aspects analyzed in their survey. Understanding the criteria and parameters used for the comparison of various electronic voting systems will provide insights into the depth and relevance of their findings.

Many articles have been written on combining blockchain technology with electronic voting systems. Research results show that each method has its own unique goals and different implementations in these articles. These publications cover a variety of methods aimed at achieving different goals using different approaches. We have not found a method of systematically mapping the literature review of electronic voting based on cryptographic protocols and blockchain technology. It is for this reason that we are conducting a systematic review of the literature for the study of electronic voting methods based on cryptographic protocols and blockchain technology to identify new trends in the industry.

According to the proposal in [14], a systematic cartographic study (SMS) was carried out using the methods of bibliometric analysis. This approach makes it possible to identify research trends, identify key topics in the field under consideration [15], and visually show the results obtained [16]. The SMS was structured in accordance with the recommendations of PRISMA (Preferred Reporting Items for Systematic Review and Meta-Analyses) [17] in the context of planning, execution, and presentation of the report. The main stages of the SMS are described in detail in the following sections. It is important to note that this study is a systematic mapping, not a literature review. There are certain differences in the final goals, research questions, the search process, and requirements for the search strategy, as well as in the evaluation of quality and results [18,19]. Unlike SLRs, research questions in SMSs are general, as their purpose is to identify research trends [20]. The research process depends on the subject area, and the search requirements are less strict since we are only interested in research trends. The quality assessment is less significant and sometimes is not carried out. The category of solution proposals includes articles without empirical evidence, as it is important to identify trends in topics. Finally, the result is an overview of the scope of the field, which allows us to identify gaps in research and trends [14].

2.1. Conducting the Search

The PRISON structure (Population, Intervention, Comparison, Outcomes, Context) used by Kitchenham and Charter [21] is applied to identify key terms and formulate search queries for the MRQ.

Population: The studies encompass electronic voting and delve into cryptographic protocols and blockchain technology.

Intervention: In our research, we explore the integration of cryptographic protocols and blockchain technology within the realm of electronic voting.

Comparison: No specific comparative analysis is undertaken in this study.

Outcomes: The study does not primarily concentrate on measurable results, as our focus lies beyond the direct outcomes of the articles.

Context: This research unfolds within an academic setting, involving the analysis of existing articles centered on electronic voting, cryptographic protocols, and blockchain technology.

As a result, the authors identified key terms within the electronic voting domain, amalgamating them into a unified search string. Subsequently, this search string underwent analysis using Web of Science (WoS) and Scopus. The constraints applied during the search process, including the search string itself, document type, language, and categories, can be referenced in Table 1. Our selection of categories was strategically limited to exclude research unrelated to this subject matter.

Table 1. Queries in the Web of Science (WoS) and Scopus search engines.

Database	Search String	Document Type	Language	Categories	Search Results
WoS	("Electronic voting" AND "Blockchain" AND "Cryptographic protocols")	article OR review	English	Computer Science OR Engineering	686
Scopus	("Electronic voting" AND "Blockchain" AND "Cryptographic protocols")	article OR review	English	Computer Science OR Engineering	468
Total 1					1154

1: In this step, duplicates are not excluded.

The study was conducted in November 2023 without limitations on the annual search range. The document type was restricted to articles and reviews, as conference materials often lack detailed information about the methods due to space constraints [22]. Additionally, conference articles are frequently supplemented by journal articles. The selection of WoS and Scopus databases for this study was based on the experience outlined in [23].

2.2. Research Selection and Quality Assessment

After downloading the search results from WoS and Scopus to Mendeley (https://www.mendeley.com/ (accessed on 17 November 2023)), a check was carried out for duplicates. The initial set of shared links was 1154 objects, of which Mendeley identified 995 unique links. After removing the duplicates, both authors reviewed the abstracts of the included articles. The following inclusion criteria (IC) and exclusion criteria (EC) were used in the analysis of abstracts:

- Request articles on electronic voting based on cryptographic protocols and blockchain technology;
- Exclude articles that, although they contain keywords for research, do not discuss the topic of electronic voting based on cryptographic protocols and blockchain technology in their abstract;
- Exclude duplicate articles, duplicate ideas presented in previous works, and exclude their annotations if they are similar. In other words, if one article is a continuation of another, the less voluminous article (with fewer pages) is excluded [24];
- Exclude articles that address common topics such as blockchain, cryptological protocols, etc., without explicitly applying them in electronic voting.

As a result, we received and transferred to VOSviewer version 1.6.20 a set of 938 relevant articles to compile a keyword map. The original set of articles, as well as separate sets of excluded and included articles, are available on GitHub (https://github.com/Tolegen95/SystLiterRW-Voting (accessed on 17 November 2023)).

The outcomes of the article selection process are illustrated in Figure 1 through a PRISMA flowchart. It is important to acknowledge that certain stages of the flowchart may deviate from the conventional PRISMA scheme given that our study is oriented towards a systematic mapping study (SMS) framework.

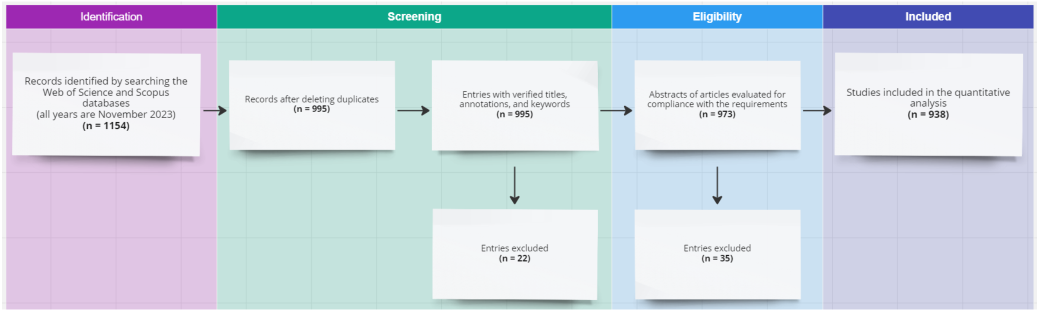

Figure 1. PRISMA block diagram (according to [17]).

2.3. Tools Used

In the course of this research, we used the following tools: (1) Mendeley to manage bibliographic references, (2) VOSviewer to analyze the bibliography and create a keyword map, and (3) Bibliometrix.

After combining the results of articles from Scopus and WoS, a situation arose where some articles were duplicates. This may be due to differences in the presentation of metadata, technical issues in merging data from different sources, or other factors that led to the re-inclusion of some publications in the final set. To ensure the accuracy and reliability of the analysis, these duplicates were then identified and removed from the research dataset using Mendeley. For further work, Bibliometrix was used to combine articles from the scientific platforms WOS and Scopus.

In their work [25–27], researchers employed various mapping tools, including VOSviewer, BibExcel, CiteSpace, CoPalRed, Sci2, VantagePoint, and Gephi, to analyze, map, and visualize bibliographic data. While a comprehensive review of visualization tools is not the primary focus of this article, we opted for VOSviewer (https://www.vosviewer.com/ (accessed on 17 November 2023)) as our analysis and mapping tool. This choice is motivated by its user-friendly and intuitive interface. VOSviewer constructs a network based on the provided bibliographic data, facilitating the exploration of relationships and patterns within the literature. For further details on VOSviewer, refer to [28]. The selection of VOSviewer is driven by its effectiveness in creating visually informative bibliometric maps, aiding us in gaining insights into the structure and connections within the electronic voting literature.

2.4. Data Extraction

To create a keyword map for electronic voting based on cryptographic protocols and blockchain technology, we used data from the conducted research, uploading titles and abstracts of articles to VOSviewer. This tool automatically selects keywords [28] and generates a map, taking into account the proximity and strength of the links between keywords based on the number of articles in which they occur together. Keywords are also grouped and displayed by color, and the size of the bubbles on the map reflects the frequency of keyword usage. VOSviewer uses a unified approach to keyword matching and clustering [29].

When creating a map based on bibliographic data or text data, data cleaning is often required [30]. To ensure consistency and accuracy in the analysis, various spellings of the same concept, such as “voting machines”, “voting system”, “voting systems”, and “e-voting system”, are harmonized. This process involves recognizing different expressions conveying a similar meaning and grouping them for a unified representation in the research dataset. Standardizing terminology enhances precision in subsequent analyses and interpretations. To accomplish this, we have developed the VOSviewer thesaurus (https://github.com/Tolegen95/SystLiterRW-Voting (accessed on 17 November 2023)), observing the following rules:

1. Combining different spellings of the same word, for example, “voting machines”, “voting system”, “voting systems”, and “e-voting system”, etc.;

2. Combining abbreviated keywords with full keywords, such as “electronic voting systems web language” and “e-voting systems”;
3. Combining synonyms, for example, “consensus mechanism” and “consensus protocols”;
4. Exclusion of common keywords such as “management”, “scheme”, “system”, etc., because they do not provide enough information.

The thesaurus includes 84 combined and excluded keywords. Finally, VOSviewer identified 3995 keywords, of which 217 occur at least five times in the titles and annotations of the selected 881 articles. The analysis of the keyword map is presented in Section 3.

2.5. The Method Used to Analyze the Results

To analyze the resulting keyword map, content analysis was used, including the following components:

1. A study of the chronological occurrence of keywords based on the analysis of their occurrence during the year (RQ-1, RQ-3).
2. An assessment of the frequency of occurrence of keywords using the Pareto distribution (80–20) [30] (RQ-2).
3. A study of the coincidence of keywords based on the analysis relationships between them (RQ-2).
4. Keyword clustering analysis using the clustering method in VOSviewer [31] (RQ-2).
5. Analysis of the occurrence and compatibility of keywords in different countries (RQ-4).

2.6. Reliability Assessment

According to [32], various types of validity are distinguished in this study, such as internal, constructive, and external. Despite careful attention being paid to the SMS process to reduce threats to credibility, we are faced with certain risks that require further discussion.

Constructive validity is applied to the concepts being studied. When analyzing the volume and keywords in the SMS, there is uncertainty as to whether the researchers referred to electronic voting about cryptographic protocols and blockchain. In this regard, a primary analysis of articles was carried out to more accurately identify keywords related to electronic voting. This demonstrates that using the keyword “electronic voting” in the search bar significantly reduces the number of possible SMS jobs, skipping important research. Therefore, common terms such as cryptographic protocols and blockchain have been included in the search bar to ensure a sufficient number of articles for the SMS. We used the WoS and Scopus databases for the search, as they provide the most relevant and high-quality peer-reviewed articles. Given the significant number of initial articles (881), we concluded that our results and discoveries are of value to researchers and practitioners, providing an overview of the current state of electronic voting based on cryptographic protocols and blockchain technology.

The threat to the internal reliability of this study is primarily related to the bias of an individual researcher when deciding whether to include or exclude articles for SMS analysis, as well as when analyzing the results. The second aspect of the threat is that most articles do not provide an accurate and direct description of the relationship between cryptographic protocols, blockchain, and electronic voting. To minimize the researcher’s bias, we applied a well-defined search strategy, carefully reviewed the titles and abstracts of the articles originally found, and also conducted a joint evaluation of the results.

Regarding external validity, it applies only to the results and conclusions of this review in the field of electronic voting. The authors have made significant efforts to systematically develop the review protocol and its application to ensure the validity of the overall conclusions, regardless of the lack of consensus.

To ensure the repeatability of our methods of systematic literature review, we have described in detail all the steps performed during the SMS, developed a thesaurus, and provided evidence of our findings (https://github.com/Tolegen95/SystLiterRW-Voting (accessed on 17 November 2023)).

3. Results

3.1. Study of Chronological Distribution (RQ-1)

Figure 2 shows the numbers of articles from 1990 to 2023 in chronological order; their total number is 938. Therefore, this time distribution allows us to answer the question RQ-1 (“What are the results of an analysis of electronic voting, cryptographic protocols, and blockchain technology research history?”). Preliminary findings indicate that research in the field of electronic voting began in 1990 and has increased markedly since 2003. This indicates the growing interest of scientists in this field of research over the past few years.

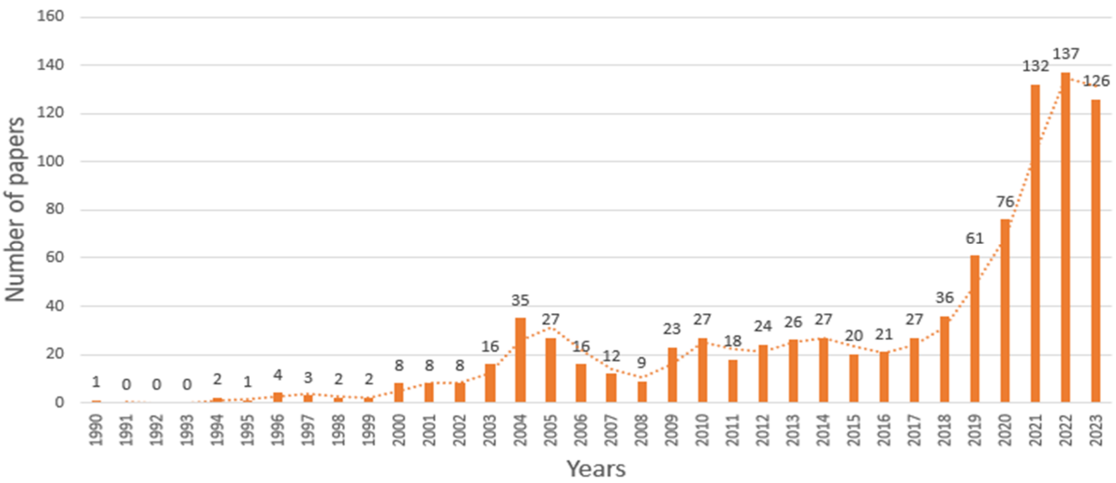

Figure 2. Temporary distribution of research in the field of electronic voting.

3.2. Research on the Frequency of Use of Keywords (RQ-2 and RQ-3)

Using the analysis methods described in Section 2.6, two keyword maps were developed in the field of electronic voting based on cryptographic protocols and blockchain technology: (1) a keyword map with the highest frequency of use (Pareto distribution—20), designed to study the most analyzed topics (RQ-2); and (2) a keyword map with an average frequency of use (Pareto distribution—80), designed to analyze the studied topics (RQ-2) and future directions (RQ-3).

3.2.1. The Most Common Keywords

The authors created a keyword map with the highest frequency of use, shown in Figure 3. To compile it, the authors set the minimum number of mentions of keywords to 11 (which corresponds to 20% of all detected keywords according to the Pareto distribution). A total of eight views and 43 keywords were highlighted that met these criteria. The 10 most frequently used keywords include electronic voting (433), security (318), cryptography (314), blockchain (281), protocol (193), privacy (149), authentication (139), networks (85), consensus (67), internet (65), and smart contract (58).

Figure 3 shows that these key terms were divided into four groups, each represented by a distinct color in the visualization. VOSviewer performs clustering based on minimizing the distances between keywords, which means that more closely related keywords are combined into one group. Therefore, the five most closely related keywords in each of these six groups are as follows: (1) algorithms, management, and consensus; (2) blockchain, decentralization, and smart contract; (3) protocol and anonymity; (3) cryptography and authentication; and (4) electronic voting, privacy, cloud computing, computer networks, and zero knowledge. It can be concluded that the first group reflects algorithms, the second group is blockchain and smart contracts, and the third group is cryptography and authentication; that is, user authentication is aimed at confirming the truth of the presented identity to make sure that this person is who he claims to be. The color scheme utilized in the visualization aids in distinguishing between these thematic clusters, providing a visual representation of the relationships between keywords within each group.

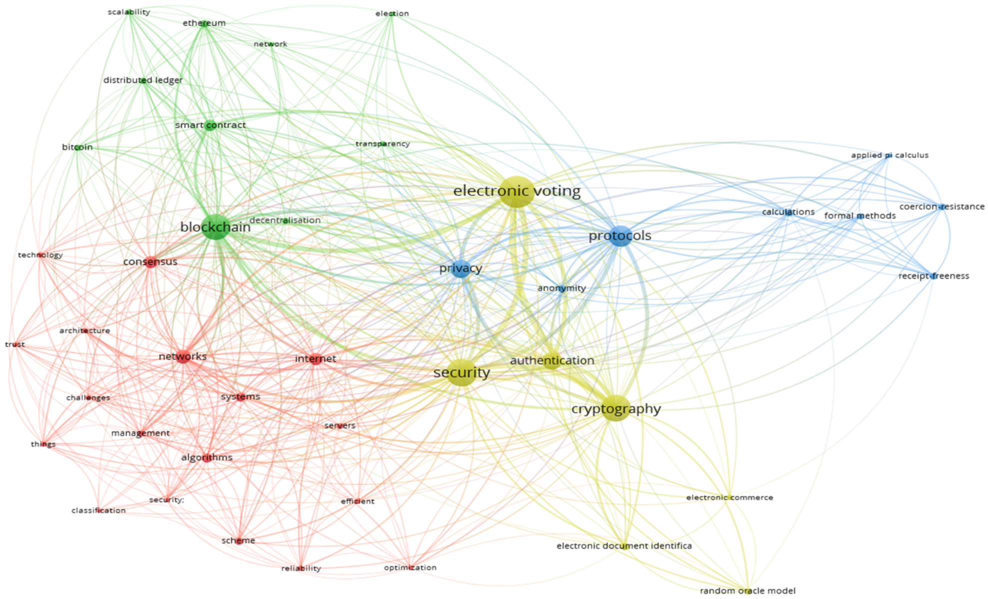

Figure 3. Graphic representation of the keywords most commonly encountered.

Figure 4 shows part of the keyword match matrix; the columns and rows of keywords in the matrix reflect the degree of co-occurrence of two key terms. In addition, the intensity of the green color indicates that keywords tend to occur together. The richer the green color, the stronger their relationship.

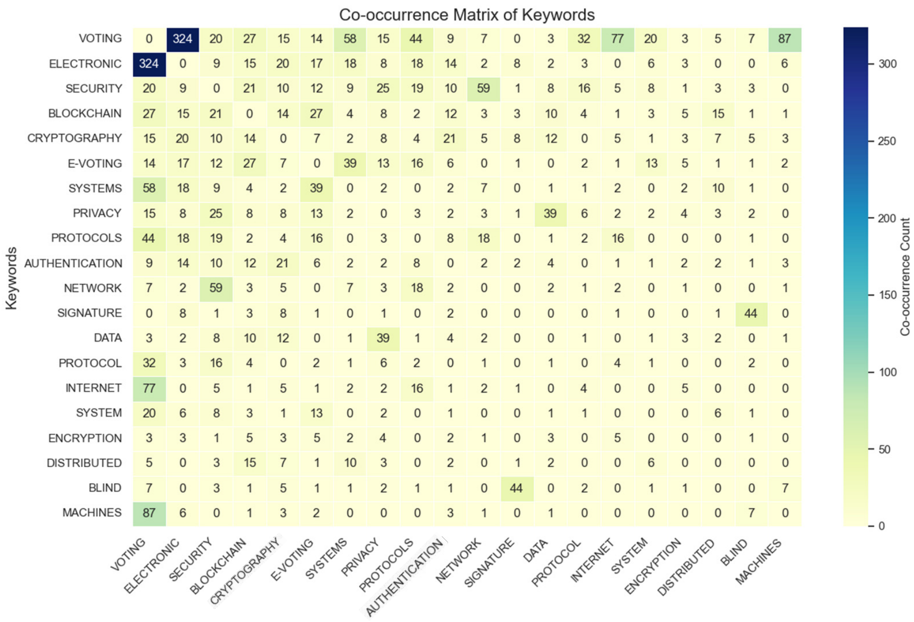

Figure 4. Matrix of coincidences of the most common key terms in the field of electronic voting.

To highlight the most common keywords, Python programming language code was implemented. The program code was then visualized using the matplotlib library version 3.7.1. It is a library for creating static, animated, and interactive graphs in the Python programming language. It is widely used for data visualization and scientific results. Matplotlib provides many functions for creating various types of graphs, charts, and maps. The corresponding fragment of the program code is shown in Figure 5.

```
# Co-occurrence matrix initialization
co_occurrence_matrix = np.zeros((num_keywords, num_keywords), dtype=int)

# Window-based Co-occurrence
window_size = 2
for i in range(len(tokens) - window_size):
    window = tokens[i:i + window_size]
    for j in range(num_keywords):
        for k in range(j + 1, num_keywords):
            if sorted_keywords[j] in window and sorted_keywords[k] in window:
                # Find the indices of the keywords in the sorted list
                index_j = sorted_keywords.index(sorted_keywords[j])
                index_k = sorted_keywords.index(sorted_keywords[k])

                # Update the co-occurrence matrix
                co_occurrence_matrix[index_j, index_k] += 1
                co_occurrence_matrix[index_k, index_j] += 1

# Create a heatmap using seaborn with improved aesthetics
sns.set(style="whitegrid")
plt.figure(figsize=(10, 8))
heatmap = sns.heatmap(co_occurrence_matrix, annot=True, fmt="d", cmap="YlGnBu", linewidths=.5,
xticklabels=sorted_keywords, yticklabels=sorted_keywords, cbar_kws={'label': 'Co-occurrence Count'})
plt.title("Co-occurrence Matrix of Keywords", fontsize=16)
```

Figure 5. Fragment of the program code.

The most common keywords are voting and electronic (324), voting and machines (87), voting and internet (77), network and security (59), voting and systems (58), and system and voting (58).

3.2.2. Keywords with a Moderate Frequency of Occurrence

A map of keywords with moderate frequency is shown in Figure 6. To create it, we limited the number of occurrences of keywords in the range from 5 to 11 (which is 80% of all detected keywords according to the Pareto distribution). VOSviewer has identified 140 keywords corresponding to the specified threshold value. The 10 most common keywords are electronic voting (433), security (318), cryptography (314), blockchain (281), protocol (193), privacy (149), authentication (139), networks (85), consensus (67), internet (65), and smart contract (58).

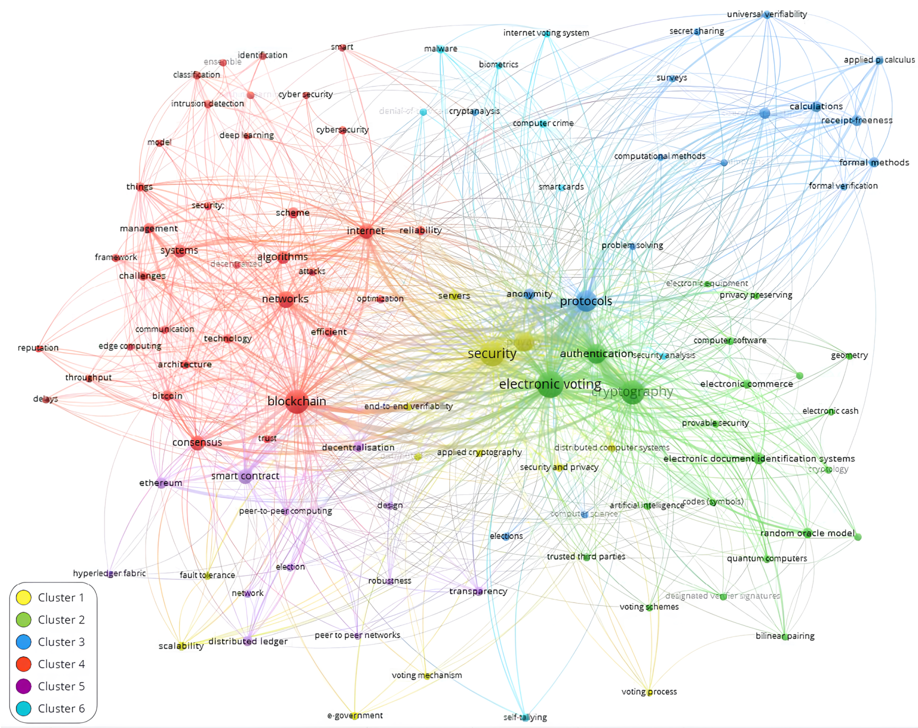

Figure 6. A map of keywords with moderate frequency.

Figure 6 shows that the key terms were distributed across six clusters. The cluster size indicates the frequency of use of a word or term in the text or its importance in the context of analysis. The cluster color can also represent additional information, such as clustering or node categorization, and also indicates different clusters or categories of terms. The closest and most common words in each cluster are (cluster 1) security, privacy, and servers; (cluster 2) electronic voting, cryptography, and authentication; (cluster 3) elections, protocols, and calculations; (cluster 4) blockchain, networks, and consensus; (cluster 5) network, smart contracts, anonymity, and optimization; (cluster 6) security analysis, malware, and biometrics. The conclusions indicate that clusters 1, 2, 3, 5, and 6 represent various applications of electronic voting based on cryptographic protocols and blockchain technology.

Figure 7 shows a fragment of the coincidence matrix of moderately common keywords in the field of electronic voting based on cryptographic protocols and blockchain technology. Rows and columns represent keywords or terms, and cell values indicate how often these keywords occur together in the analyzed texts. Below are the keywords or terms that occur in the analyzed texts with an average frequency. This helps us to understand which terms are related to each other and which concepts are closely interrelated.

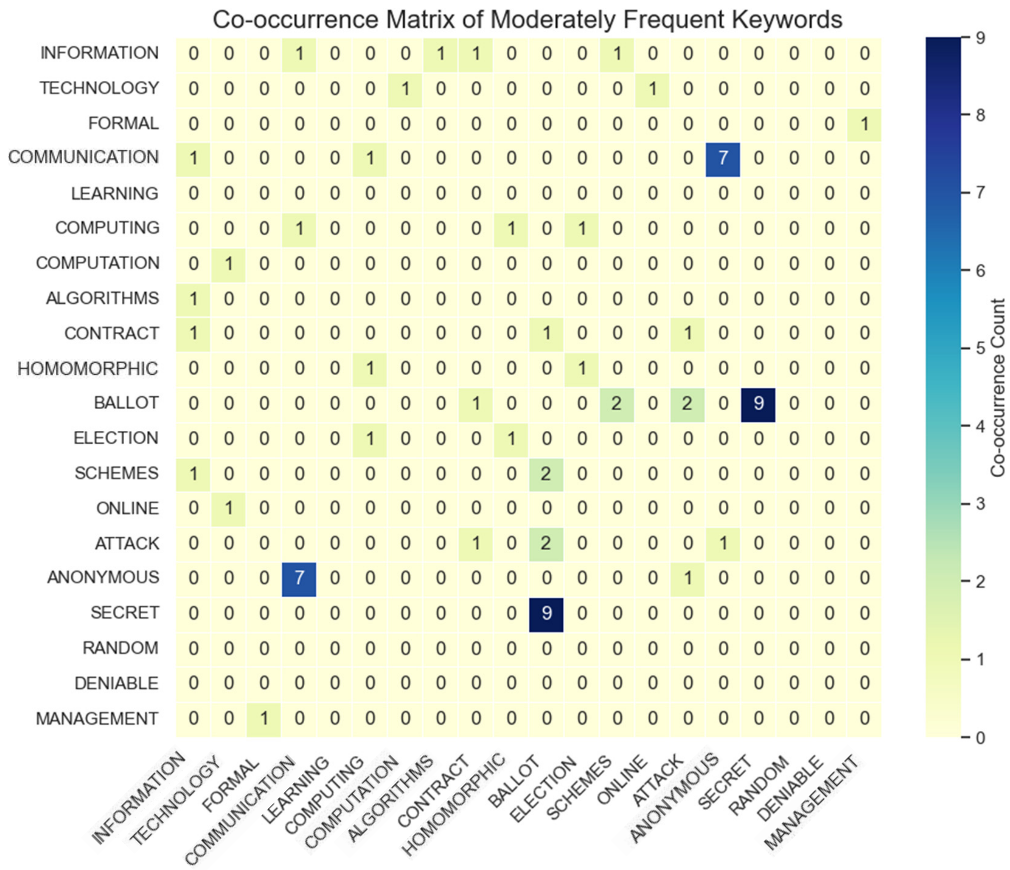

Figure 7. Matrix of co-occurrence of moderately frequent keywords in the field of electronic voting.

As can be seen, the most common keywords are the following: secret and ballot (9), communication (7), and ballot and attack (2). Therefore, it can be concluded that to search for semantically rich information, it is necessary to use a semantic extension of the query.

Identifying such data helps researchers understand which topics and concepts are most closely related in the field of electronic voting. This can help identify the main topics and problems in this area, identify the connections between different concepts, and identify the most relevant terms for further study or analysis. It can also help researchers identify potential areas for further research or development.

Figure 8 shows the distribution of keywords that occur with moderate frequency, depending on the average publication year (APY). The APY indicates the average year of publication of documents containing the specified keywords. A moderate frequency of keyword usage in different years allows us to identify which terms and concepts have remained relevant over time and which have appeared or disappeared. For further research, this helps to identify trends and changes in the use of terminology in a particular area of knowledge over time. Currently, special attention is paid to the analysis of such topics in the field of blockchain, smart contracts, consensus (APY 2020), authentication, privacy, networks (APY 2018), electronic voting, calculations, voting schemes (APY 2016), cryptography, protocols, efficiency (APY 2014), protocols, security, elections (APY 2012), computer software, cryptology, and electronic commerce (APY 2010).

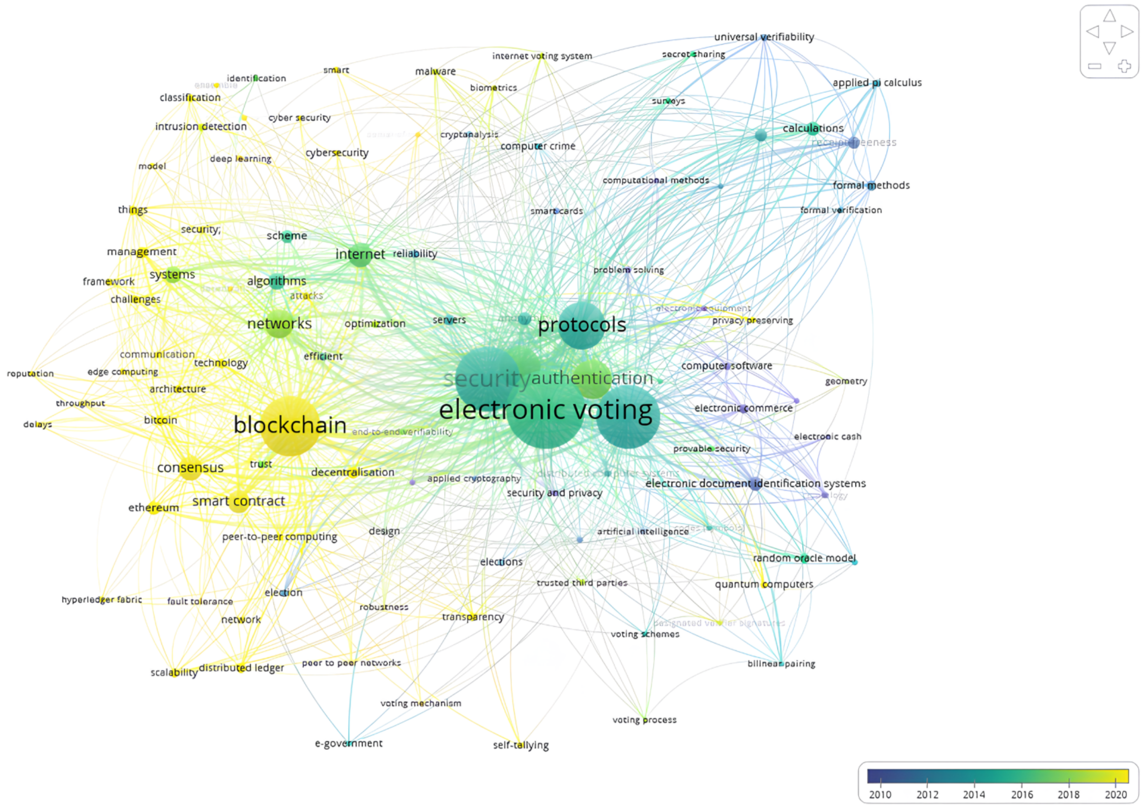

Figure 8. A map showing a moderate frequency of keyword usage in different years.

3.3. The Countries Participating in the Study Are Considered (RQ-4)

To analyze the activity of countries in the field of electronic voting based on cryptographic protocols and blockchain technology (RQ-4), we have created two maps of countries' participation in WoS and Scopus. It is worth noting that these maps were developed separately from each other to identify differences in WoS and Scopus. This was necessary due to the variety of search models, query parameters, limited library scanning capabilities, limited access to bibliographic information of articles, inconsistency of search models in digital libraries, and differences in formatting (such as author names and country names).

Figure 9 shows a map of countries created from WoS data on electronic voting based on cryptographic protocols and blockchain technology. The five countries that stand out most on the map include the People's Republic of China (197), the USA (115), India (68), England (43), and Australia (41). The values next to the countries indicate the number of documents published by each country.

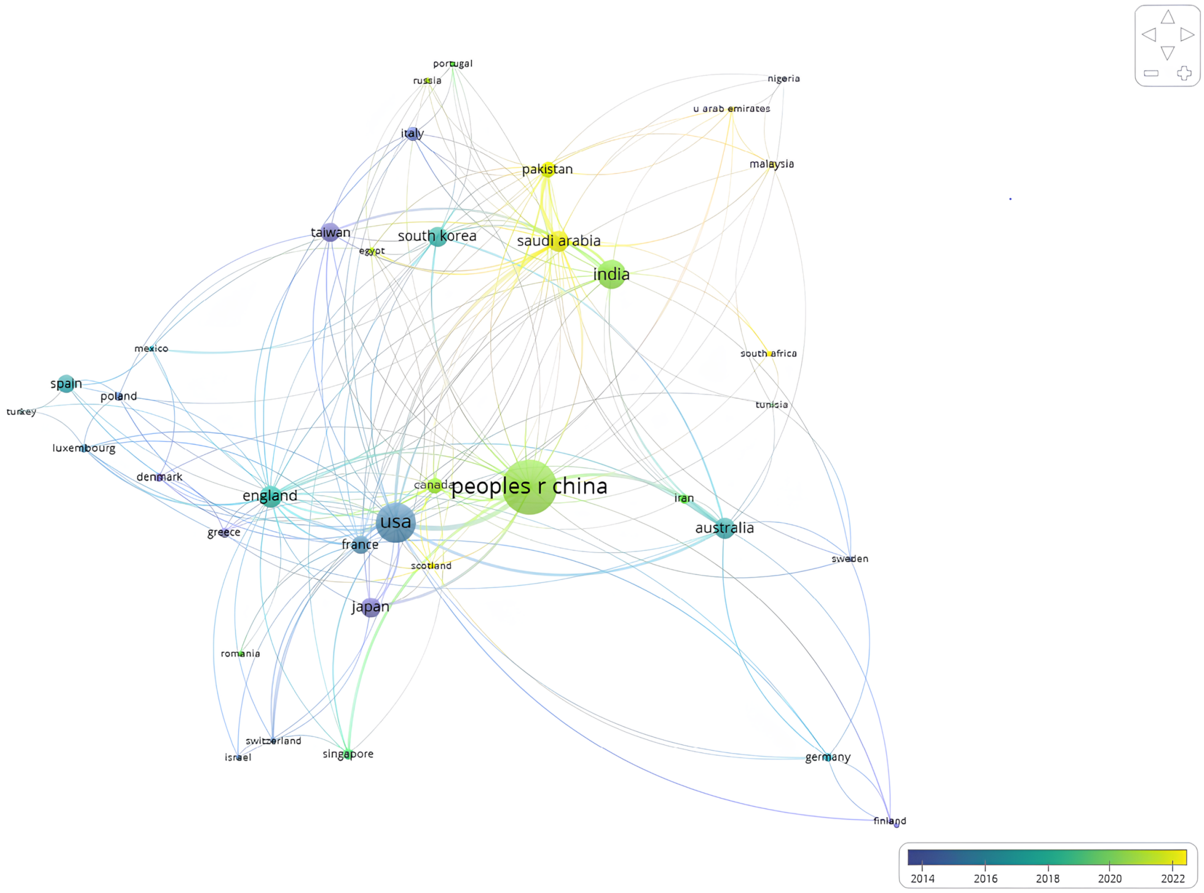

Figure 9. Map of countries in the context of electronic voting created using WoS.

In this image, the countries are colored according to the APY, which reflects the average year of publication of documents issued by each country. Visualization is a network map where each country is represented as a node, and connections between countries can indicate cooperation and interactions in the field of electronic voting.

The countries highlighted in yellow represent innovators in this field of research, namely Saudi Arabia (2022 y.), Pakistan (2021 y.), the People's Republic of China (2021 y.), and Malaysia (2020 y.). Their contribution to the topic of electronic voting based on cryptographic protocols and blockchain technology is relatively recent, which is reflected in their recent appearance in the APY rating.

Visualization of this data helps researchers to better understand international cooperation and interaction between countries in the field of electronic voting and identify the main participants, as well as possible trends or patterns in the distribution of scientific papers on this topic.

Table 2 shows a matrix of comparison of countries according to WoS data. The columns and rows of the matrix represent countries, and the cells contain information about the degree of overlap between the two countries. An empty cell indicates that there is no connection between countries. The intensity of the green color indicates that certain countries tend to appear together. The more intense the green color, the higher the degree of coincidence. For example, the following countries are highlighted, which are often found in the context of RQ-4: China and the USA (25), China and Australia (13), and Saudi Arabia and Pakistan (10).

Table 2. Compliance with the Web of Science countries in the field of electronic voting based on cryptographic protocols and blockchain technology.

Countries	**Australia**	**Canada**	**Egypt**	**India**	**Japan**	**Korea**	**Luxembourg**	**Malaysia**	**Pakistan**	**Saudi Arabia**	**Singapore**	**United Kingdom**	**USA**
China	13	8		9	7	5			4	9	9	8	25
France												5	
India	5									9			
Korea	4												
Saudi Arabia			4					4	10				
United Kingdom		4					4		6				
USA	7	6		5						8		7	

The intensity of green color shows countries appearing together. Stronger green means higher coincidence.

Figure 10 shows a map of countries in the context of electronic voting based on cryptographic protocols and blockchain technology developed based on data from Scopus. The five most common countries on this map include China (95), India (68), the USA (49), Taiwan (39), and the UK (33). It is worth noting that the top five countries most commonly found in Scopus coincide with those that are present in WoS, except for the order of their location.

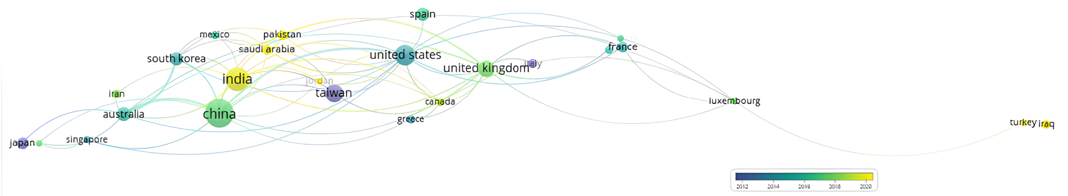

Figure 10. A map of countries related to the topic of electronic voting based on data from Scopus.

In Figure 10, countries are highlighted according to the APY. The size and color of the nodes may indicate various characteristics, such as the number of publications, citations, or the importance of each country in a given context. New countries that have contributed to this area of research are marked in yellow. These include Pakistan (2020), China (2018), the USA (2016), South Korea (2014), and Taiwan (2012). Compared to WoS, in Scopus, two countries are the same (Pakistan, China) and two differ (Australia and USA). Countries with a high volume of documents, such as China, Spain, Italy, and the UK, have an APY distributed in the middle of the year.

In Table 3, the columns and rows of the matrix represent countries, and the cells display the degree of overlap between them. Empty cells indicate that there are no links between countries. The intensity of the green color indicates that countries tend to appear together, with a richer green color indicating a stronger mutual inclusion. According to the data (RQ-4), the most common countries are China and Australia (7), China and the USA (7), China and India (5), and also Korea and Australia (5).

Table 3. The mutual presence of countries in Scopus in the field of electronic voting based on cryptographic protocols and blockchain technology.

Countries	Australia	Canada	France	Germany	Hong Kong	India	Korea	Luxembourg	Pakistan	Romania	Saudi Arabia	Singapore	South Africa	United Kingdom	USA
Canada								2							
China	7	3			2	5	2				2	3		3	7
France				2						2					
India	3	2					3				3		2	3	2
Korea	5														
Pakistan											3				
United Kingdom			3	3					5						
USA											3				

The intensity of green color shows countries appearing together. Stronger green means higher coincidence.

4. Discussion

Electronic voting, based on cryptographic protocols and blockchain technology, is an advanced field combining innovations to ensure the security, transparency, and efficiency of the electoral process. In this context, the use of cryptographic protocols and blockchain technology gives electronic voting several advantages.

1. Cryptographic protocols:

Data security: The use of cryptographic methods ensures a high level of protection of voter data. Encryption and signatures ensure the confidentiality and integrity of votes.

Identification and authentication: Cryptography allows us to effectively solve the issues of identification and authentication of voters, minimizing the risks of fraud.

2. Blockchain technology:

Immutability and transparency: The blockchain creates an immutable chain of blocks where each vote is part of a distributed registry. This guarantees transparency and eliminates the possibility of tampering with the results.

Decentralization: Due to the decentralized nature of the blockchain, the electronic voting system becomes less susceptible to centralized attacks and manipulations. In conclusion, we will discuss the results of the SMS.

As part of this study, we used systematic mapping with bibliometric analysis methods to answer the main research question (MRQ): How does the use of cryptographic protocols and blockchain technology contribute to electronic voting? From the MRQ, the following research questions (RQs) are formulated: RQ-1: What are the results of an analysis of electronic voting, cryptographic protocols, and blockchain technology research history? RQ-2: What aspects are being considered for the study of electronic voting based on cryptographic protocols and blockchain technology? RQ-3: What is the main direction of the future development of the topic under study? RQ-4: What is the experience and level of progress of various countries in the deployment of electronic voting systems using cryptographic protocols and blockchain technology?

This systematic cartographic study (SMS) on the topic of EV, based on cryptographic protocols and blockchain technology, shows a significant increase in the number of articles since 2003 (RQ-1). This can be explained by technological development and the increasing applicability of these technologies in various fields.

To answer RQ-2, the authors applied the frequency of occurrence, performed keyword clustering using VOSviewer, and wrote Python code to analyze the co-occurrence of keywords. In addition, the authors studied the developed maps of the frequency of occurrence of keywords using the Pareto distribution. The map of the most common keywords (Pareto distribution—20) allowed us to identify the main topics of EV based on cryptographic protocols and blockchain technologies, such as electronic voting, security, cryptography, and blockchain. Cluster analysis of this map revealed four main areas: (1) algorithms, (2) blockchain, (3) protocols, and (4) electronic voting considering the context and rules. The matrix of coincidences confirms these conclusions.

A map of keywords with a moderate frequency of occurrence (Pareto distribution—80) allowed us to identify subtopics (RQ-2) of the main topics (Pareto distribution—20) and consider possible future directions (RQ-3). The analysis of the frequency of occurrence of keywords and clustering revealed various applications of EV based on cryptographic protocols and blockchain technology. The co-occurrence matrix confirms that the search, storage, and analysis of data require the expansion of traditional electronic voting to secure electronic voting.

Keywords with a moderate frequency of occurrence, as identified through the analysis of patterns of keywords (APY), play a pivotal role in predicting potential future directions within the realm of electronic voting (EV) based on cryptographic protocols and blockchain technologies. Uncovering keywords like "learning", "random", "management", etc., with moderate frequency provides valuable insights into emerging trends and focal points in the field. This section is deemed one of the most crucial components, shedding light on areas that warrant further exploration and contributing significantly to shaping the trajectory of research and development in EV.

The authors analyzed two separate country maps for WoS and Scopus to study notable trends in research in the field of EV based on cryptographic protocols and blockchain technology (RQ-4). The results obtained on the WoS country map and the Scopus country map are very similar. In general, the most common countries were the People's Republic of China, the USA, India, England, and Australia. Pakistan, China, the USA, South Korea, and Taiwan have recently contributed. Countries that are most often found in pairs include China and Australia, China and the USA, and China and India, as well as Korea and Australia. From this, it can be concluded that the People's Republic of China, the USA, India, England, and Australia occupy leading positions in the field of EV based on cryptographic protocols and blockchain technology, and research is expanding to new countries. The authors also noted that the leading countries in this area have close international ties, which is evident from the matrix of coincidences. Thus, we can conclude that international cooperation allows us to develop the topic and increase its popularity.

To sum up, cryptographic protocols and blockchain contribute to the field of information security by expanding traditional electronic voting (MRQ) to secure systems capable of changing the use of electronic voting in different countries.

Another noteworthy advantage and outcome of this study lies in the utilization of two prominent scientific databases, namely WoS and Scopus. This dual-database approach enhances our ability to observe overarching trends with a sufficient level of precision. Notably, the construction of separate country maps for WoS and Scopus reveals a congruence in trends among countries actively engaged in research on electronic voting based on cryptographic protocols and blockchain technology. From this observation, it can be inferred that to gain a broad understanding of this field within a concise timeframe, employing a single scientific database may suffice. However, for a more comprehensive investigation, it is advisable to leverage multiple data sources, such as WoS and Scopus.

Based on the received answers to the research questions, we came to a deeper understanding of the field of EV based on cryptographic protocols and blockchain technology. This stimulates further research directions for more effective development of EV. However, more in-depth methods should be applied in future research, such as the study of joint citations and co-authorship and the expansion of the research area to other scientific databases.

Building upon the comprehensive analysis presented in the discussion section, we further explore the implications of our findings and their significance for the field of electronic voting (EV) based on cryptographic protocols and blockchain technology.

Implications of the results:

Our systematic mapping study (SMS) revealed a substantial increase in research articles on EV, cryptographic protocols, and blockchain technology since 2003. This trend underscores the growing interest and recognition of these technologies' potential to revolutionize the electoral process.

Through meticulous keyword clustering and co-occurrence analysis, we unravel the intricate web of topics within the realm of EV. The identification of key areas such as algorithms, blockchain, protocols, and electronic voting processes provides valuable insights into the multifaceted nature of research in this domain, guiding future investigations.

Keywords with moderate frequency shed light on emerging trends, such as the integration of machine learning and advanced management techniques. These findings hint at the evolving landscape of EV towards more sophisticated and resilient voting systems.

Significance for the field:

Our study highlights the crucial role of cryptographic protocols and blockchain technology in fortifying the security, transparency, and efficiency of electronic voting systems. By leveraging encryption, digital signatures, and blockchain's immutable ledger, we address concerns surrounding data integrity and trust in electoral processes.

The utilization of both Web of Science (WoS) and Scopus databases underscores the importance of comprehensive data analysis in discerning global research trends. This approach not only elucidates overarching patterns but also emphasizes the interconnectedness of countries engaged in EV research, fostering a collaborative environment for innovation.

Furthermore, our examination of international collaboration underscores the significance of knowledge exchange and partnership among researchers worldwide. The synergy observed among leading countries in EV research reflects a collective commitment to advancing the field and fostering innovation on a global scale.

Future research directions:

While our study provides valuable insights, there are avenues for further exploration. Future research endeavors could employ advanced methodologies, such as joint citations and co-authorship analysis, to elucidate collaboration networks and research impact more comprehensively.

Expanding the scope of our research to include other scientific databases can offer a more holistic understanding of global research trends and emerging areas of interest. Exploring interdisciplinary connections and integrating diverse perspectives can enrich our understanding of the multifaceted challenges and opportunities in EV.

In conclusion, our study contributes significantly to the ongoing discourse on EV based on cryptographic protocols and blockchain technology. By delving into the implications of our findings and their broader significance, we aim to catalyze further research and innovation, ultimately advancing the development of secure, transparent, and efficient electronic voting systems worldwide.

5. Conclusions

In the course of this study, a systematic cartographic study (SMS) was conducted with a bibliometric analysis on the topic of electronic voting (EV) based on cryptographic protocols and blockchain technology. As a result, a keyword map was created that provides a systematic view of the topic and reflects its main ideas.

An analysis of the chronological distribution of articles on EV based on cryptographic protocols and blockchain technology revealed a significant increase in publications since 2003, indicating the relevance and extensive research of this topic.

During the analysis of the most common keywords, the focus of the research was highlighted, including electronic voting. Cluster analysis of the keyword map identified the main areas in EV: algorithms, blockchain, and protocols.

The analysis of keywords with moderate frequency allowed us to identify various applications of EV based on cryptographic protocols and blockchain technology.

According to API data, the analysis of moderately occurring keywords allowed us to anticipate possible development trends in the field of EV based on cryptographic protocols and blockchain technology.

It is noted that this SMS provided quantitative results based on keyword analysis. To obtain new perspectives and discover new areas of research in the field of EV, it is also recommended to conduct a systematic review of the literature with quantitative and qualitative studies in the future.

Another important achievement of this SMS is the use of two scientific databases, WoS and Scopus, which allowed us to observe more extensive trends with high accuracy and draw more generalized conclusions. In addition, an analysis of the participation of various countries in research on EV based on cryptographic protocols and blockchain technology in WoS and Scopus showed similar trends and developments.

Author Contributions: Conceptualization, D.S., N.G. and T.A.; methodology, N.G.; software, T.A.; validation, N.G., D.S. and A.N.; formal analysis, T.A.; investigation, T.A.; data curation, T.A.; writing—original draft preparation, T.A.; writing—review and editing, N.G.; visualization, T.A.; supervision, D.S.; project administration, A.N.; funding acquisition, A.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research is funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP19175746).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data relevant to the research are provided at https://github.com/Tolegen95/SystLiterRW-Voting (accessed on 17 November 2023).

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Baudier, P.; Kondrateva, G.; Ammi, C.; Seulliet, E. Peace engineering: The contribution of blockchain systems to the e-voting process. *Technol. Forecast. Soc. Chang.* **2021**, *162*, 120397. [CrossRef]
2. Kim, T.; Ochoa, J.; Faika, T.; Mantooth, A.; Di, J.; Li, Q.; Lee, Y. An overview of cyber-physical security of battery management systems and adoption of blockchain technology. *IEEE J. Emerg. Sel. Top. Power Electron.* **2020**, *10*, 1270–1281. [CrossRef]
3. Hang, L.; Kim, D.-H. Design and implementation of an integrated IoT blockchain platform for sensing data integrity. *Sensors* **2019**, *19*, 2228. [CrossRef]
4. Chang, V.; Baudier, P.; Zhang, H.; Xu, Q.; Zhang, J.; Arami, M. How Blockchain can impact financial services–The overview, challenges and recommendations from expert interviewees. *Technol. Forecast. Soc. Chang.* **2020**, *158*, 120166. [CrossRef]
5. Hjálmarsson, F.Þ.; Hreiðarsson, G.K.; Hamdaqa, M.; Hjálmtýsson, G. Blockchain-Based E-Voting System. In Proceedings of the IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; pp. 983–986.
6. Berenjestanaki, H.; Barzegar, H.R.; El Ioini, N.; Pahl, C. Blockchain-Based E-Voting Systems: A Technology Review. *Electronics* **2024**, *13*, 17. [CrossRef]
7. Chun, F.L.; Ngai, E.W.T. Blockchain from the information systems perspective: Literature review, synthesis, and directions for future research. *Inf. Manag.* **2023**, *60*, 103856.
8. Webster, J.; Watson, R.T. Analyzing the past to prepare for the future: Writing a literature review. *MIS Q.* **2002**, *26*, 13–23.
9. Steininger, D.M. Linking information systems and entrepreneurship: A review and agenda for IT-associated and digital entrepreneurship research. *Inf. Syst. J.* **2019**, *29*, 363–407. [CrossRef]
10. Wareham, J.G.; Zheng, D. Straub Critical themes in electronic commerce research: A meta-analysis. *J. Inf. Technol.* **2005**, *20*, 1–19. [CrossRef]
11. Dubé, L.; Paré, G. Rigor in information systems positivist case research: Current practices, trends, and recommendations. *MIS Q.* **2003**, *27*, 597–636. [CrossRef]
12. Berdik, D.; Otoum, S.; Schmidt, N.; Porter, D.; Jararweh, Y. A Survey on Blockchain for Information Systems Management and Security. *Inf. Process. Manag.* **2020**, *58*, 102397. [CrossRef]
13. Xiao, S.; Wang, X.A.; Wang, W.; Wang, H. Survey on blockchain-based electronic voting. In Proceedings of the International Conference on Intelligent Networking and Collaborative Systems, Victoria, BC, Canada, 31 August–2 September 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 559–567.
14. Petersen, K.; Vakkalanka, S.; Kuzniarz, L. Guidelines for conducting systematic mapping studies in software engineering: An update. *Inf. Softw. Technol.* **2015**, *64*, 1–18. [CrossRef]

15. Ramaki, A.A.; Rasoolzadegan, A.; Bafghi, A.G. A Systematic Mapping Study on Intrusion Alert Analysis in Intrusion Detection Systems. *ACM Comput. Surv.* **2018**, *51*, 1–41. [CrossRef]
16. Linnenluecke, M.K.; Marrone, M.; Singh, A.K. Conducting systematic literature reviews and bibliometric analyses. *Aust. J. Manag.* **2020**, *45*, 175–194. [CrossRef]
17. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G.; The PRISMA Group. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Med.* **2009**, *6*, e1000097. [CrossRef]
18. Zhang, C.; Budgen, D. What Do We Know about the Effectiveness of Software Design Patterns? *IEEE Trans. Softw. Eng.* **2011**, *38*, 1213–1231. [CrossRef]
19. Kitchenham, B.A.; Budgen, D.; Brereton, O.P. Using mapping studies as the basis for further research—A participant-observer case study. *Inf. Softw. Technol.* **2011**, *53*, 638–651. [CrossRef]
20. Kalibatiene, D.; Miliauskaite, J. A Systematic Mapping with Bibliometric Analysis on Information Systems Using Ontology and Fuzzy Logic. *Appl. Sci.* **2021**, *11*, 3003. [CrossRef]
21. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Technical Report EBSE 2007-001; Keele University: Keele, UK; Durham University: Durham, UK, 2007.
22. Dybå, T.; Dingsøyr, T. Empirical studies of agile software development: A systematic review. *Inf. Softw. Technol.* **2008**, *50*, 833–859. [CrossRef]
23. Kalibatienė, D.; Miliauskaitė, J.A. Hybrid Systematic Review Approach on Complexity Issues in Data-Driven Fuzzy Inference Systems Development. *Informatica* **2021**, *32*, 85–118. [CrossRef]
24. Kitchenham, B. *Procedures for Performing Systematic Reviews*; Joint Technical Report TR/SE-0401; Keele University: Keele, UK; Australian Technology Park: Sydney, Australia, 2004; pp. 1–26.
25. Cobo, M.; Martínez, M.; Gutiérrez-Salcedo, M.; Fujita, H.; Herrera-Viedma, E. 25 years at Knowledge-Based Systems: A bibliometric analysis. *Knowl. Based Syst.* **2015**, *80*, 3–13. [CrossRef]
26. Zhu, Q.; Kong, X.; Hong, S.; Li, J.; He, Z. Global ontology research progress: A bibliometric analysis. *Aslib J. Inf. Manag.* **2015**, *67*, 27–54. [CrossRef]
27. Vilutiene, T.; Kalibatiene, D.; Hosseini, M.R.; Pellicer, E.; Zavadskas, E.K. Building Information Modeling (BIM) for Structural Engineering: A Bibliometric Analysis of the Literature. *Adv. Civ. Eng.* **2019**, *2019*, 5290690. [CrossRef]
28. Van Eck, N.J.; Waltman, L.; Noyons, E.C.M.; Buter, R.K. Automatic term identification for bibliometric mapping. *Science* **2010**, *82*, 581–596. [CrossRef] [PubMed]
29. Khalil, G.; Gotway Crawford, C. A bibliometric analysis of US-based research on the behavioral risk factor surveillance system. *Am. J. Prev. Med.* **2015**, *48*, 50–57. [CrossRef]
30. Van Eck, N.; Waltman, L. *Manual for VOS Viewer*; Version 1.6.10; CWTS, Universiteit Leiden: Leiden, Holland, 2019.
31. Adeniji, B.A. Bibliometric Study on Learning Analytics. Master's Thesis, Long Island University, New York, NY, USA, 2019.
32. Waltman, L.; Van Eck, N.J.; Noyons, E.C. A unified approach to mapping and clustering of bibliometric networks. *J. Inf.* **2010**, *4*, 629–635. [CrossRef]