Blockchain Security Research Progress and Hotspots

Ke Yuan, Yingjie Yan, Lin Shen, Qian Tang*, *Member, IAENG,* and Chunfu Jia

***Abstract*—Blockchain is poised to advance the cause of product innovation and technology evolution as a novel decentralized infrastructure and distributed computing model. However, there are serious security risks in the blockchain itself, which will restrict the development of blockchain and related applications. To better grasp the current status of blockchain security research and explore the research hotspots and frontier, this study used Citespace as a bibliometric analysis tool to collect 3993 research papers between 2014 and 2020 from the WoS Core Collection as a data sample. We conduct a comprehensive overview of blockchain security research in terms of authors, research institutions, publications, countries, citations and keywords in a visual graph. This paper shows that the literature record continues to be refreshed, and it peaked in 2019. China and the USA are the main regions for collaborative research. They have established partnerships with many countries whose research institutions and authors play an important role in the collaborative network. Blockchain security research hotspots are mainly related to "cryptocurrency", "supply chain", "smart contract", "healthcare", "consensus mechanism", "fog computing", "cyber attack" and "Internet of Thing (IoT)". The lineage of blockchain development has evolved from an early focus on cryptocurrency and blockchain security risk analysis to securing other areas, such as financial systems, the IoT and healthcare through blockchain. In the future, blockchain security research will be combined with much newer technologies to form diverse developments.**

***Index Terms*—Blockchain Security, Bibliometric Analysis, Research Hotspots.**

I. Introduction

THE blockchain system is a special kind of distributed database consisting of various technologies, such as cryptography, peer-to-peer (P2P) network, consensus mechanism and smart contract. Cryptographic techniques include hashing algorithms, asymmetric encryption algorithms, digital certificates, digital signatures, and other encryption techniques, which guarantee confidentiality, integrity, authentication and non-repudiation of data. Unlike the central network system that has a central server, P2P network is an internet system without a central node which means each node in it can be either a client or a server. The consensus mechanism is the core value of blockchain technology, that is, there is no central node, and each node jointly maintains a distributed ledger. There are several commonly used consensus mechanism, such as proof-of-work, proof-of-stake, and Byzantine consensus algorithms. The smart contract is an immutable script stored on the blockchain. The content of a smart contract is encoded, and the contract program is executed automatically when the conditions for the trigger agreement are met.

Blockchain's value is increasing as the theoretical research progresses. However, the blockchain continues to reveal security issues, such as scalability, anonymity, and security threats. Blockchain has become an obvious target for attacks [1]. In 2010, hackers launched an attack against Bitcoin, exploiting a significant integer overflow vulnerability to create 184,467 million Bitcoins [2] out of thin air. In 2016, the attackers managed to steal 12 million Ether [3] from 30% of decentralized autonomous organizations (DAOs) contracts. In June 2018, two South Korean exchanges suffered attacks on their hot wallets, with financial losses of up to 71 million USD [4]. Researchers and developers have begun to conduct research and development related to blockchain security.

A large body of relevant literature has emerged to provide a specific and systematic overview of blockchain security research. Zhu et al. [5] provided a comprehensive classification and summary of blockchain data security. Bonneau et al. [6] focused on investigating the security and privacy of cryptocurrency and Bitcoin. Atzei et al. [7] demonstrated and analyzed the vulnerabilities in a smart contract, and provided a taxonomy of common programming pitfalls that lead to vulnerabilities.

Bibliometrics [8] is a cross-cutting discipline that uses mathematical and statistical methods to quantitatively analyze all carriers of knowledge. Statistical analysis of the year, country, and institution of publication can be used to determine the spatial and temporal distribution of the literature, and collaborative network analysis can demonstrate institutional and author collaborations, while co-citation analysis can be performed to obtain high-impact authors and literature. Keyword analysis can identify research hotspots and frontiers. Bibliometrics scientifically demonstrates the structure and trends of academic fields. It is necessary to conduct an insight analysis of blockchain security, discover its knowledge structure, research hotspots and frontiers, provide valuable references for subsequent related research.

This study used bibliometric software (Citespace) to conduct spatio-temporal analysis, highly-citation literature analysis, collaborative network analysis, co-citation analysis, cluster analysis and co-occurrence analysis of the literature

Manuscript received May 20th, 2021; revised January 29th, 2022. This work was supported by the National Key R&D Program of China under Grant 2018YFA0704703; the National Natural Science Foundation of China under Grant 61972215, 61802111 and 61972073; the Key Research and Promotion Projects of Henan Province under Grant 222102210062; the Basic Research Plan of Key Scientific Research Projects in Colleges and Universities of Henan Province under Grant 22A413004.

Ke Yuan is an Associate Professor of School of Computer and Information Engineering, Henan University, Kaifeng, 475004, China; Henan Key Laboratory of Big Data Analysis and Processing, Henan University, Kaifeng, 475004, China (e-mail: yuanke@henu.edu.cn).

Yingjie Yan is a postgraduate student of School of Computer and Information Engineering, Henan University, Kaifeng, 475004, China (e-mail: yanyingjie@henu.edu.cn).

Lin Shen is an undergraduate student of School of Computer and Information Engineering, Henan University, Kaifeng, 475004, China (e-mail: shenlin@henu.edu.cn).

Qian Tang is an Associate Professor of College of Geography and Environmental Science, Henan University, Kaifeng, 475004, China (corresponding author to provide e-mail: tangqian_rubia@163.com).

Chunfu Jia is a Professor of College of Cybersecurity, Nankai University, Tianjin, 300350, China (e-mail: cfjia@nankai.edu.cn).

on blockchain security research in the Web of Science (WoS) core collection over the past seven years.

II. Data and Methods

A. Data Sources

With its strict selection mechanism, the Web of Science is an essential database for accessing global academic information. It covers more than 15,000 authoritative and influential academic journals worldwide in natural sciences, engineering and technology, biomedicine, social sciences, arts and humanities. Based on Garfield's Law of Concentration in bibliometrics, it includes only the most essential scholarly papers in each discipline and research field. The WoS core collection was selected as the target database for searching source literature. The search formula was set to TS = (Blockchain) AND TS = (safety OR security OR risk). And our search was conducted for selection from 2014 to 2020 (as of December 31st, 2020), a total of 3993 search records were obtained.

B. Methods and Tools

Collaborative network analysis, co-citation analysis, co-occurrence analysis and cluster analysis were conducted on 3993 documents through the visualization software, Citespace [9]. When performing co-citation and co-occurrence analysis, the strength of the connections between network nodes must be calculated based on the number of co-citations or co-occurrences of the generated network. In general, there are three methods used to calculate the strength of connections in a network, and they are Cosine, Jaccard and Dice, as given in equations (1), (2) and (3), respectively.

$$Cosine(c_{ij}, s_i, s_j) = \frac{c_{ij}}{\sqrt{s_i, s_j}} \tag{1}$$

$$Jaccard(X, Y) = \frac{X \bigcap Y}{X \bigcup Y} \tag{2}$$

$$Dice(c_{ij}, s_i, s_j) = \frac{c_{ij}}{s_i + s_j} \tag{3}$$

Cluster analysis is a technique used to group sets of objects with similar characteristics. It takes an unsupervised learning mode, and the document data can be analyzed by setting certain distances, similarity formulae, and clustering iteration thresholds. The construction of two text vectors to be compared is the core of document clustering analysis. The classical algorithms are Term frequency-inverse document frequency (TF-IDF) and its various improvements and weighting algorithms. In these algorithms, TF indicates the frequency of specific words or phrases appearing in the document, as shown in equation (4), while IDF can filter some generic words, as shown in equation (5).

$$tf_{i,j} = \frac{n_{i,j}}{\sum_{k=1}^{j} n_{k,j}}. \tag{4}$$

$$idf_j = \log \frac{n_{i,j}}{1 + |j : t_i \subseteq d_j|} \tag{5}$$

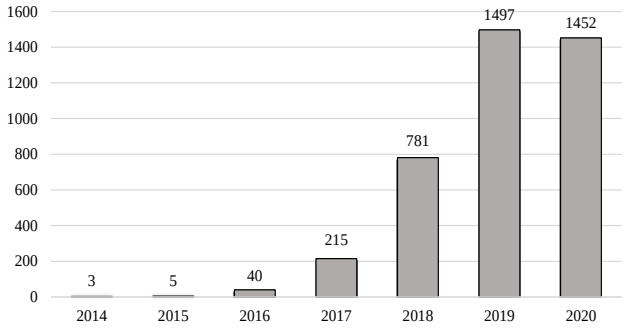

Fig. 1. Trends in the growth of the literature

TABLE I
Distribution of publication types

Type of Document	Count	Proportion %
Article	2038	51.04
Proceedings Paper	1724	43.18
Review	203	5.08
Early Access	158	3.96
Book Chapter	36	0.9

III. Results and Discussion

A. Literature Distribution

1) Time Distribution of the Literature: A total of 3993 papers related to blockchain security research were retrieved from the Web of Science core collection database, covering the years from 2014 to December 2020. The annual distribution of literature is shown in Fig.1. The development of blockchain security research can be divided into two phases.

Initial phase (2014-2015): Blockchain security research started to take off in 2014 and it was not until 2015 that research literature reached 5 articles. During this stage, the main topic was the security of digital cryptocurrency. Eyal et al. [10] pointed out that incompatible Bitcoin mining protocols can lead to insecure mining. It can be seen that early research focused on Bitcoin security and privacy.

Development phase (2016-2020): During the period from 2016 to 2020, the amount of literature increased rapidly. Scholars paid considerable attention to the safety of blockchain, and relevant studies in this field increased. Blockchain security research entered the development stage.

2) Type Distribution of the Literature: There are five publication types in the 3993 papers, along with their corresponding numbers and proportions. As shown in Table I, the articles are the largest proportion, which contains 2038 papers. There are also 1724 conference papers, 203 reviews, 158 early access and 36 book chapters.

3) Disciplinary Distribution of the Literature: The disciplinary distribution of research literature helps in understanding the disciplinary structure of the research field. The top 8 disciplinary field categories for blockchain security research are shown in Fig.2. These categories included Computer Science (2465), Engineering (1571), Telecommunications (1137), Business Economics (265), Chemistry (116), Science Technology Other Topics (97), Automation Control Systems (87) and Medical Informatics (73). Blockchain security research covers several different fields, among which Computer Science, Engineering, and Telecommunications are the critical fields of research. In short, blockchain security research

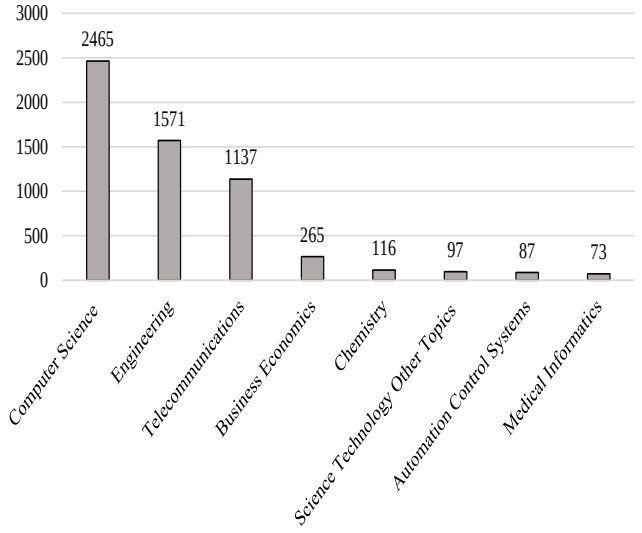

Fig. 2. Top 8 disciplinary categories in blockchain security research

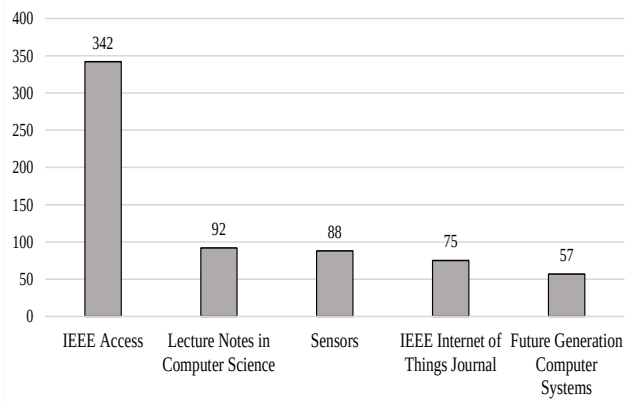

Fig. 3. Top 5 publications distribution of blockchain security research

is multidisciplinary and interdisciplinary.

4) Distribution of Publications in the Literature: Academic journals promote the exchange, dissemination and inheritance of scientific research. The top 5 publications in terms of the number of journals were obtained through Citespace's analysis of primary source publications in the research field, as shown in Fig.3. These journals were IEEE Access (342), Lecture Notes in Computer Science (92), Sensors (88), IEEE Internet of Things (IoT) (75) and Future Generation Computer Systems (57). All five publications are related to computer science.

5) Growth Trends in the Number of Institutions, Countries, Authors, Publications: The growth trend of the total number of publications, authors, institutions and countries from 2014 to 2020 is shown in Fig.4. The figure shows that the number of countries, authors, scientific institutions and publications related to blockchain security research grew in recent years and reached its peak in 2019.

B. Cooperation Network Analysis

1) Author cooperation analysis: Citespace was used to analyze the data for collaboration networks. Some author nodes that did not have a collaboration network were removed. A total of 576 authors had established collaborations. The nodes represent the authors, the connecting lines

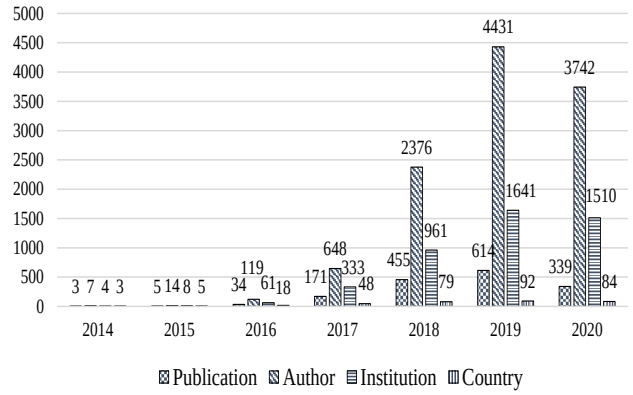

Fig. 4. Growth trends in growth in the number of Institutions, Countries, Authors, and Publications

TABLE II
LITERATURE PRODUCTION AND CENTRALITY OF THE TOP 10 AUTHORS

Authors	Year	Count	Centrality
Kimkwang Raymond Choo	2018	37	0.20
Mohsen Guizani	2017	30	0.21
Neeraj Kumar	2018	30	0.21
Xiaojiang Du	2017	29	0.03
Jong Hyuk Park	2017	27	0.00
Khaled Salah	2018	23	0.04
Sudeep Tanwar	2018	20	0.00
Debiao He	2018	18	0.07
Yan Zhang	2017	18	0.10
Hui Li	2017	16	0.03

represent the collaboration between the authors, the width of the connection represents the strength of the collaboration, and the clustering yielded 7 color blocks, namely, 7 clusters(shown in Fig.5). For example, Bodkhe et al. [11], He et al. [12] and Alladi et al. [13] were the most frequent collaborators whose research interests were IoT security. Xia et al. [14] and Li et al. [15] were collaborators whose research interests were cryptographic technology game theory. Xia et al. [16] and Khan et al. [17] focused on blockchain privacy protection research.

The top 10 authors who had the most published papers along with their country, research institution, frequency, and centrality are shown in Table II. In the development stage of blockchain security research, Choo was the most published author with a centrality of 0.20. Guizani had a centrality of 0.21, indicating that his publications were related to multiple papers and act as a "traffic hub". Choo collaborated with others on research related to the privacy protection of blockchain healthcare data [18] and on the security of blockchain IoT [19].

2) Institutions Cooperation Analysis: A collaborative network analysis of 185 research institutions was conducted through Citespace and clustered to obtain 7 color blocks, namely, 7 clusters. The nodes represent research institutions, the size of the nodes represents the number of publications, and the connecting lines represent the collaboration between institutions (shown in Fig.6). For example, King Saud University [20] and Comsats University Islamabad in Pakistan [21], had frequent cooperation, and their research focused on consensus mechanism security. Beijing University of Posts and Telecommunications [22] and Beijing University of Aeronautics and Astronautics (Beihang Univ) [23] led

Fig. 5. Author Collaboration Network Analysis.

research collaboration with a bias toward blockchain cybersecurity. The collaboration of Xian University of Electronic Science and Technology [24] and Wuhan University [25] was focused on Bitcoin security. Shanghai Jiaotong University [26] was a primary research institution with a research bias toward blockchain key management. The collaboration between the institutions led by Asia University [27] and the Thapar Institute of Engineering and Technology [28] was relatively weak and focused on blockchain smart grids. Table III shows the frequency and centrality of the top 20 institutions. Of the 20 research institutions, there were 18 universities and 2 national institutes. This indicates that universities were the mainstay of blockchain security research. Among the 18 universities, 12 were from China, 2 from North America, 2 from West Asia, 1 from Australia and 1 from South Asia. Of the 2 national research institutes, one was from China and the other from Australia. Beijing University of Posts and Telecommunications (76), the University of Electronic Science and Technology of China (62) and the Chinese Academy of Sciences (61) ranked in the top three in terms of literature, and all of them had high centrality. This indicates that Chinese research institutions published a high volume of literature and collaborated relatively frequently with other institutions.

3) Analysis of National Cooperation Networks: A collaborative network with 102 nodes and 642 links is shown in Fig.7, where the size of the nodes indicates the number of articles published in different countries and the number of links indicates the frequency of collaboration in each country. The larger the node, the more articles are published, and a high centricity of nodes implies their significance. China and the USA are at the center of the graph and are important nodes.

The order of centrality in Table IV is as follows: South Korea < India < Italy = Germany = Saudi Arabia < China = Canada < Australia < England < USA. The maximum value of centrality for the USA is 0.21. This indicates that many countries such as the USA, England and Australia maintained extensive academic collaboration, while China had the highest number of publications and less collaboration with other countries. Most of these are developed countries, mainly in Europe and North America.

TABLE III
LITERATURE PRODUCTION AND CENTRALITY OF THE TOP 20 AUTHORS

Institution	Count	Centrality
Beijing Univ Posts & Telecommun	76	0.08
Univ Elect Sci & Technol China	62	0.08
Chinese ACAD Sci	61	0.07
Xidian Univ	58	0.07
Univ TEXAS SAN ANTONIO	46	0.08
King SAUD Univ	41	0.08
Shanghai Jiao Tong Univ	38	0.07
CSIRO	37	0.06
Beihang Univ	36	0.06
Beijing Inst Technol Univ	35	0.02
Nanyang Technol Univ	32	0.04
Temple Univ	32	0.02
Qatar Univ	32	0.04
Univ Technol Sydney	31	0.05
Wuhan Univ	31	0.07
Chinese ACAD Sci Univ	30	0.01
Tsinghua Univ	29	0.06
Guangdong Univ Technol	29	0.03
Hong Kong Polytech Univ	29	0.04
Huazhong Univ Sci & Technol	28	0.04

TABLE IV
LITERATURE PRODUCTION AND CENTRALITY IN THE TOP 9 COUNTRIES

Countries	Count	Centrality
China	1187	0.08
USA	782	0.21
India	346	0.04
England	262	0.20
South Korea	251	0.02
Australia	240	0.13
Canada	186	0.08
Italy	143	0.06
Germany	142	0.06

C. Co-Citation Analysis and High-Citation Literature Analysis

1) Co-citation Analysis of the Literature: Two (or more) papers are said to be co-cited if they are both cited by a later paper [29]. The higher co-citation frequency of two authors, the closer their scholarly relationship is. Co-citation analysis of literature was conducted using Citespace. As shown in Fig.8, there are 417 nodes and 1983 edges in the citation network. The largest connected branch accounts for 92% of the total nodes. Therefore, most literature had established citation relationships, which were then analyzed by clustering, resulting in 7 clusters, namely, 7 color blocks.

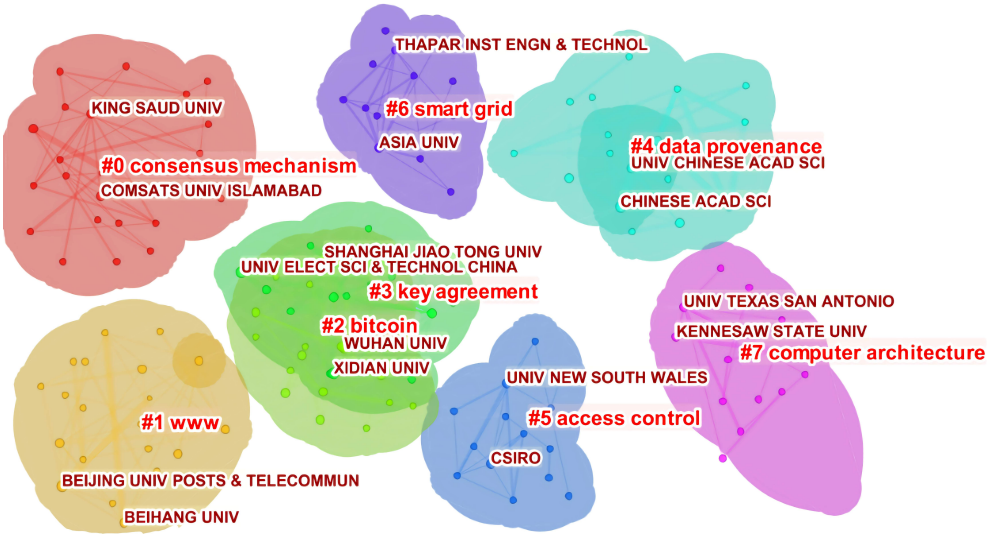

Fig. 6. Institutional cooperation network analysis.

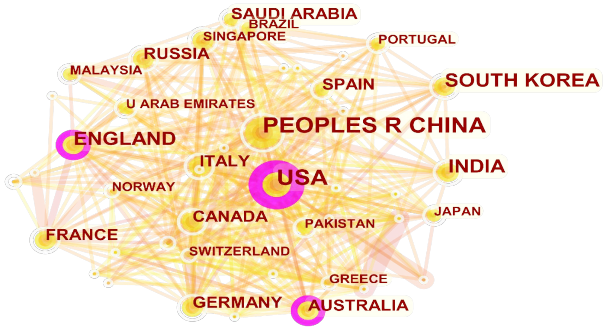

Fig. 7. Analysis of country cooperation networks

For example, Swan [30] described the concepts, features and functions of Bitcoin and blockchain in detail. Hawk [31] is a programming language for creating a privacy-preserving smart contract that allows for safe privacy transactions. Azaria et al. [32] used blockchain to address the protection of e-health systems.

2) Total Co-Citation Analysis of Publications: Publication co-citation analysis is widely used in multidisciplinary research fields. As shown in Fig.9, the nodes represent publications and the lines between the nodes represent the relationships between publications. Co-citation analysis is performed on publications. There were 365 publications with co-citation relationships, and seven clusters were obtained through cluster analysis. The red section is about Bitcoin and consists mainly of publications such as Lecture Notes in Computer Science [33, 34]. The yellow section is about fog computing and consists mainly of publications such as, Future Generation Computer System [35–37]and IEEE Access [38–40]. The purple section is about microgrids and consists mainly of publications such as, Applied Energy [41, 42] and IEEE Transactions on Smart Grid [43, 44].

3) Analysis of High-Citation Literature: Highly-citation literature is innovative and important and has some research significance. Table V lists the top 10 highly-citation references, along with the citation frequency and percentage. One study [1],which is the originator of blockchain research, first introduced the concept of Bitcoin and gave its complete architecture. Zyskind et al. [45] first transformed blockchain into an automated access control manager that does not require trusting third parties to store, query and share data. Zheng [46] gave an overview of blockchain and then compared some typical consensus used in different blockchain algorithms. Wood [47] presented a novel blockchain system, the Ethernet platform, which used smart contract to make blockchain integration with other domains a reality. Azaria et al. [32] were the first to propose a programmable and privacy-preserving smart contract model, where traditional blockchain transactions were public, however, Hawk hid the details of user transactions. Khan and Salah [48] analyzed and classified the major IoT security problems,and explained how blockchain might help solve many of these issues.

IV. RESEARCH HOTSPOTS AND FRONTIER ANALYSIS

A. Research Hotspots Analysis

In general, keywords represent the main research directions of the literature, which reflect important information such as the core ideas and themes of the literature. Citespace was used to perform cluster analysis of keywords. A total of 6529 keywords were selected. Table VI shows the top 20 keywords, frequency and centrality. Among them, blockchain and security are in an absolute position. To improve the security of blockchain systems, the most closely involved parts of blockchain security research are IoT, smart contract, networks, and Bitcoin. Figure 10 shows the hot topics of this period categorized into 8 areas based on the objective statistical results of the cluster analysis and eliminates irrelevant and repetitive clustered words.

Cryptocurrency: Cryptocurrency is usually based on blockchain as the underlying technology, and in the case of Bitcoin, [49] pseudonyms are used to achieve anonymity for transactions.To improve Bitcoin anonymity, Saxena et al. [50] proposed a method using a composite signature that removes all links between the sending and receiving addresses of a transaction. Bitcoin-NG [51] has Byzantine fault tolerance for optimal scalability. Karame [52] analyzed Bitcoin attacks and threats and described and evaluated counter-measures

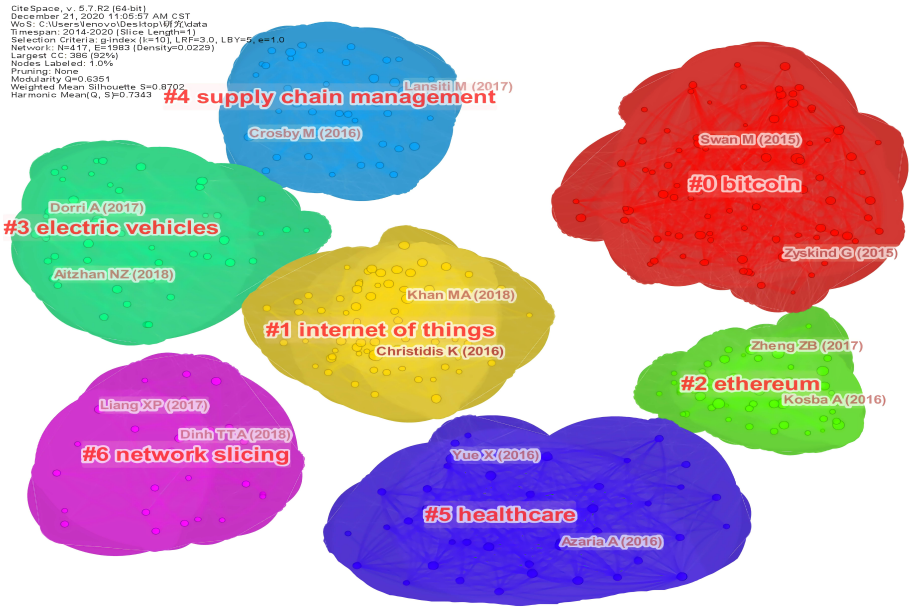

Fig. 8. literature co-citation analysis.

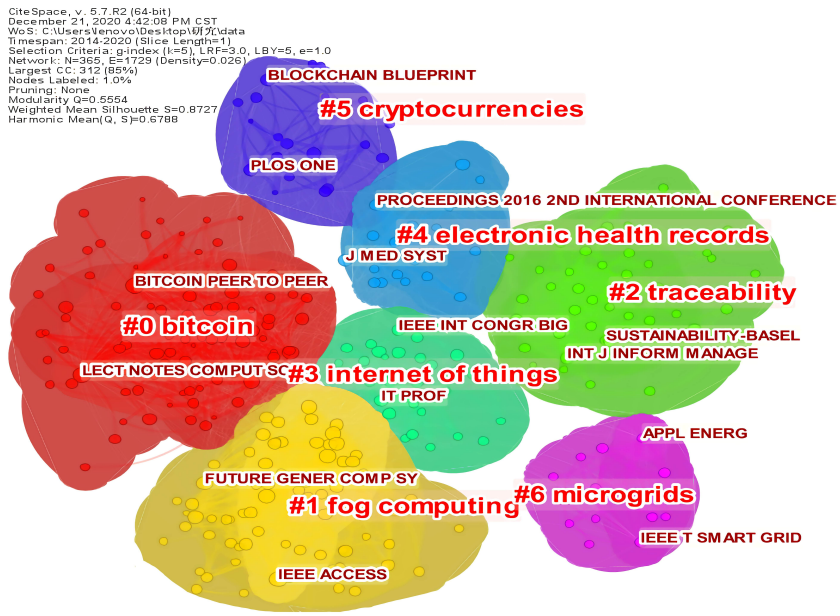

Fig. 9. Total co-citation analysis of publications.

to better design and analyze the next generation of secure blockchain currencies.

Supply chain: The use of blockchain technology helps to deal with exceptions and quickly trace items back through each link in the supply chain. Blockchain systems allow multiple agencies and organisations to share information about the supply chain. In the supply chain, the radio-frequency identification technology is widely used, but it can also be easily copied. Toyoda et al. [53] proposed a blockchain-based supply chain application platform that makes it difficult to clone authentic tags. In comparison to the traditional supply chain systems, Tse et al. [54] proposed an application of blockchain for information security in the food supply chain with tamper-evident and traceable properties.

Smart contract: The stability of smart contract is vital to Ethereum's operation. Luu et al. [55] created Oyente, a symbolic execution notation tool, to record smart contract vulnerabilities and address the seriousness of attacks. Bhargavan et al. [56] developed a system for monitoring and verifying the security and usefulness of smart contracts when they are in use. By detecting odd token sequences and optimizing current deep analyzers, Liu et al. [57] proposed S-gram, a novel semantic-aware security auditing methodology that can predict future smart contract vulnerabilities.

Healthcare: By overcoming information silos in healthcare data between organizations and improving the efficiency of healthcare management while protecting patients, blockchain technology can address the shortcomings of the traditional healthcare industry. The MedRec system [32] offered users a novel, decentralized blockchain medical records management system in which all the logs were detailed and permanent. Ancile [58] addressed privacy and security issues in the healthcare sector by providing interoperable access to medical information, patients, data vendors, and third parties.

TABLE V
TOP 10 HIGH-CITATION REFERENCES.

Title	Author	Year	Journal	Count
Bitcoin: A peer-to-peer electronic cash system	Nakamoto	2008	Dectentralized Business Review	1173
Blockchains and smart contract for the internet of things	Christidis et al	2016	IEEE Access	462
Decentralizing Privacy: Using blockchain to protect personal data	Zyskind et al	2015	IEEE Security and Privacy Workshops	285
Blockchain: Blueprint for a new economy	Swan	2015	Blockchain Blueprint	276
Ethereum: A secure decentralised generalised transaction ledger	Wood	2014	Ethereum Project Yellow Paper	246
An overview of blockchain technology: Architecture, consensus, and future trends	Zheng et al	2017	International Conference on Open and Big Data	237
Practical byzantine fault tolerance	Castro et al	1999	Usenix Symposium on Operating System Design and Implementation	222
Medrec: Using blockchain for medical data access and permission management	Azaria et al	2016	International Conference on Open and Big Data	206
Hawk: The blockchain model of cryptography and Privacy-preserving smart contracts	Kosba et al	2016	IEEE Symposium on Security and Privacy	206
Blockchain challenges and opportunties:A survey	Zheng et al	2018	International Journal of Web and Grid Services	204

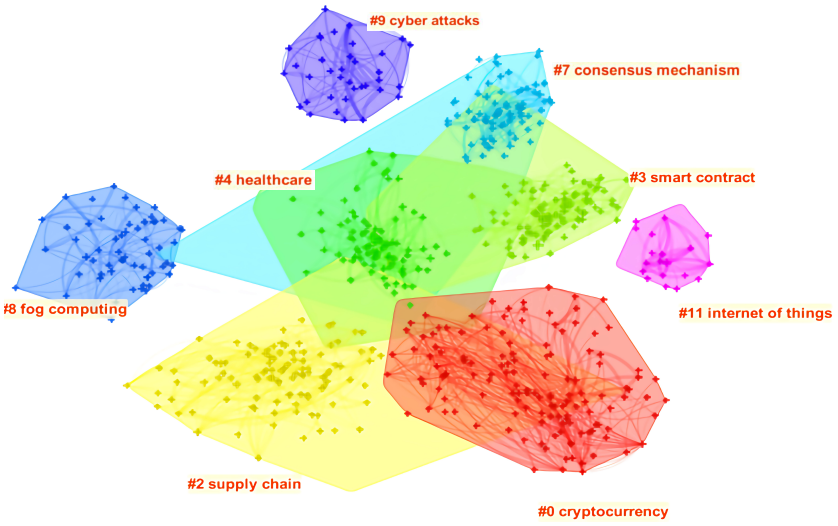

Fig. 10. Keyword co-occurrence analysis.

TABLE VI
TOP 20 KEYWORDS OF THE BLOCKCHAIN SECURITY STUDIES.

Rank	Keywords	Occurrences	Centrality
1	Blockchain	2703	0.05
2	Security	896	0.03
3	Internet of Thing	837	0.03
4	Smart contract	597	0.04
5	Internet	512	0.03
6	Privacy protection	464	0.05
7	Bitcoin	286	0.06
8	Consensus mechanism	246	0.04
9	Cloud	214	0.05
10	Authentication	187	0.03
11	Distributed ledger	184	0.02
12	Cryptocurrency	178	0.04
13	Ethereum	178	0.01
14	Computer architecture	169	0.02
15	Technology	164	0.04
16	Challenge	163	0.03
17	Trust	156	0.04
18	Access control	142	0.05
29	Supply chain	123	0.03
20	Healthcare	117	0.03

Healthchain [59] combined the IoT, medical devices, and blockchain electronic medical records to secure the privacy of data on IoT devices.

Consensus mechanism: The performance and reliability of the consensus structures extracted from Bitcoin and Ether are no longer adequate for evolving federated blockchain. By crowd-sourced polling, Li et al. [60] proposed a new accuracy algorithm, Proof of Voting, with managed protection and low latency. The CapserFFG consensus mechanism, proposed by Xian et al. [61] , detectes attackers by comparing the dubious scores of all verifiers. De et al. [62] proposed a blockchain-driven trust system based on the blockchain's credibility. A miner's credibility worth must be greater than a certain level for him to begin mining, or he will be kicked off the blockchain system. Bou et al. [63] proposed PL-PoRX, a permissionless proof-of-reputation algorithm that reduces the number of blocks created by malicious miners while assisting benevolent miners.

Fog computing: By providing localized computing, storage, and networking for IoT devices, fog computing increases resource management constraints and security. Almadhoun et al. [64] proposed a user authorization system in which fog nodes communicate with Ethereum smart contracts to verify users' identities while using IoT computers. Tu et

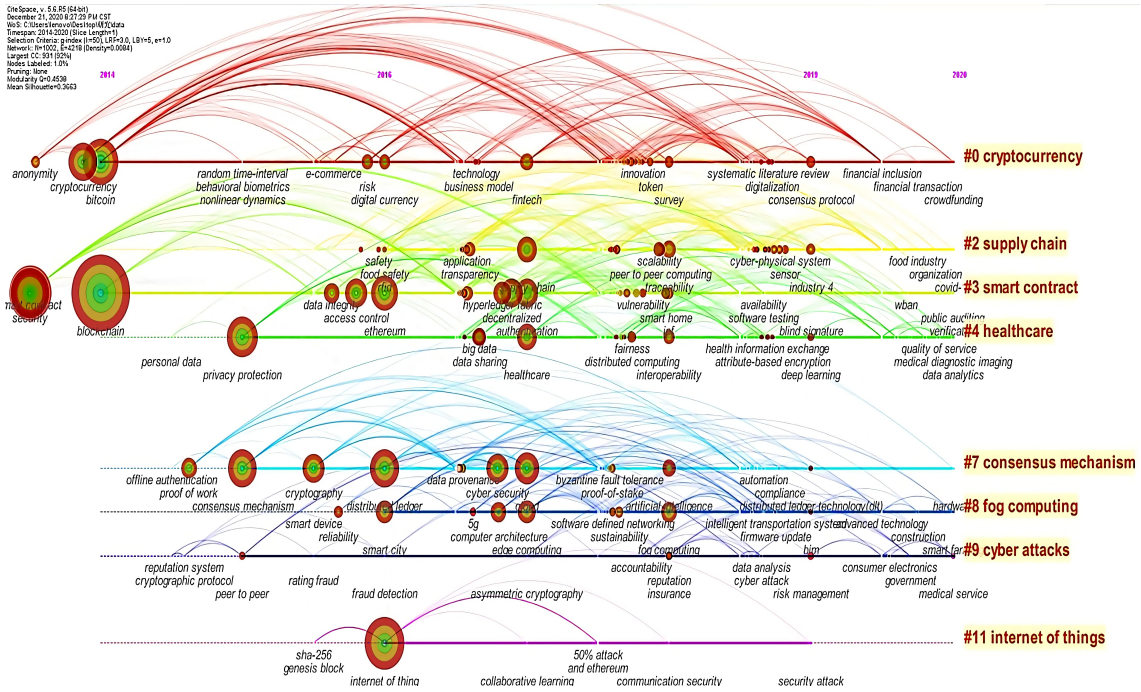

Fig. 11. Timeline view of blockchain security keywords.

TABLE VII
TOP 15 KEYWORDS WITH THE STRONGEST CITATION BURSTS.

Keywords	Year	Strength	Begin	End	2014 - 2020
Bitcoin	2014	14.45	2014	2017	
Cryptocurrency	2014	4.1	2014	2018	
Digital currency	2014	5.13	2016	2017	
Cryptography	2014	3.07	2016	2017	
E-Commerce	2014	2.98	2016	2018	
Food safety	2014	1.48	2016	2017	
Distributed ledger	2014	4.95	2017	2018	
Data provenance	2014	3.56	2017	2018	
Identity	2014	2.36	2018	2020	
Solidity	2014	2.19	2018	2020	
Rfid	2014	2.02	2018	2020	
Rigital economy	2014	1.69	2018	2020	
Internet of Thing	2014	1.52	2018	2020	
Fog	2014	1.52	2018	2020	
Efficienty	2014	1.52	2018	2020	

al. [65] introduced a FogBus architecture that incorporated various IoT systems into fog and cloud infrastructures. Edge and remote tools can be used to deploy, track, and control IoT applications. Ho et al. [66] proposed a blockchain-based mobile cloud system that could perform cloud computing and other functions through mobile terminals, and it could also be interconnected with virtual terminals.

Cyber attack: Blockchain technology can help organizations prevent single points of failure, mitigate cyber attack, and make it impossible for malicious attackers to steal or tamper with business data. Toapanta et al. [67] proposed a database security model test prototype that mitigated cyber attack with security effectiveness of 99.5 percent. Raban et al. [68] assessed the usefulness of emerging technologies for cyber security defense, stating that blockchain and cryptographic primitives would aid in improving defense capabilities and classifying emerging technologies for evaluation. The possibilities of blockchain technology in enhancing cyber security were discussed in prior work [69].

Internet of Thing: Blockchain technology has been widely applied to IoT [70] to provide infrastructure support and help solve the widespread security problems of IoT. Huh et al. [71] used Ethereum smart contract to manage the IoT system in a more granular manner. Sharma et al. [72] proposed a new blockchain-based distributed cloud architecture that provides low-cost, secure and on-demand access to the most competitive computing infrastructure in IoT. Petcon [73] used incentives to perform electric vehicle purchases, ensuring the confidentiality of transactions without the use of third parties. Sharma et al. [74] proposed a distributed vehicle network architecture that runs in a distributed manner to build a new distributed transmission management system. Yang et al. [75] proposed a system to verify the management of information generated from nearby vehicles.

In summary, the hotspots of blockchain security research include the basic knowledge of blockchain and other fields of science and technology. The initial focus was on cryptocurrency security research, which later shifted to using blockchain technology to ensure the security of other technologies.

B. Frontier Analysis

The timeline view focuses primarily on sketching the relationships between clusters and the historical span of literature in a given cluster. Fig.11 shows a timeline diagram that approximately illustrates the analysis of hot topics in blockchain security from 2014 to 2020. Time is the horizontal axis, the nodes are keywords, and the connecting lines between the nodes show the relationships between the keywords. The bigger the nodes, the more common the keywords are.

In the initial stage (2014 to 2015), the research was mainly focused on "bitcoin", "smart contract", "cryptocrrency" and "privacy protection". These started to become the hotspots of blockchain security research. Since entering the growth stage (2016 to 2020), clusters like "smart contract", "healthcare", "consensus process", "fog computing", "IoT" and others have begun to gain attention. Each cluster's nodes are connected, indicating that the eight research hotspots are associated. The research hotspots were initially the security of cryptocurrencies like Bitcoin and Ether, while later the focus shifted to the application of blockchain technology in other domains to protect their security.

The top 15 keywords with the strongest citation bursts are shown in Table VII, with "bitcoin" (14.45) having the highest outbreak rate, followed by "digital currency" (5.13). The increased number of Bitcoin-related research hotspots from 2014 to 2017 has contributed to the high severity of the Bitcoin and digital currency outbreak. In blockchain security analysis, emerging technologies such as "solidity", "digital economy" , "IoT" and "fog" are at the forefront.

V. Conclusion

Using the visualization software Citespace, this paper conducts an econometric analysis of the literature on blockchain security research from 2014 to 2020. Literature distribution, author contributions, research hotspots, and research frontiers are among the main contents. The knowledge structure, research hotspots and frontiers of blockchain security in the period are identified through plotted collaborative network analysis, co-citation analysis, and co-occurrence and timeline graphs.

The main conclusions can be summarized as follows. Blockchain security research can be divided into two phases according to the temporal distribution: the initial phase (2014 to 2015) and the development phase (2016 to 2020). China had the largest number of publications in blockchain security research, while the USA was the second largest. The main research disciplines in blockchain security research were computer science, engineering applications and communications and other engineering fields. A complete system of cooperation had been formed between research institutions and authors in each country, and Chinese research institutions and authors were the mainstays of research. The direction of cooperation among research institutions was mainly the consensus mechanism, network, key, data traceability and computer system. Moreover, the collaborative research among authors tended to be in the direction of IoT, game theory, privacy protection, and artificial intelligence.

The co-citation literature can be divided into 7 clusters: Bitcoin, fog computing, IoT, healthcare, cryptocurrency, reliability, and networking. Journals with high citations were extracted from the categories of core journals in the field, namely, IEEE Access, IT Professional, and Applied Energy. The most cited literature was Satoshi Nakamoto's Bitcoin, which became the first successful application of blockchain technology. Ethereum laid the groundwork for the development of blockchain and made its commercial application possible.

By analyzing the high-frequency keywords, blockchain security research hotspots were cryptocurrency, supply chain, smart contract, healthcare, consensus mechanism, fog computing, cyber attack and IoT. In the initial stage, the research hotspots were biased toward the security of cryptocurrency, vulnerability attacks, and blockchain security. In the development stage, with the continuous maturity of smart contract technology, blockchain was combined with other technologies to secure the supply chain, healthcare, and IoT. With the emergence of technologies, such as 5G and quantum computers, the future of blockchain security will accelerate.

Focusing on the knowledge structure and research progress of blockchain security research, this paper proposes a systematic analysis method, obtains knowledge architecture, and research hotspots and frontier. However, there are still some shortcomings in this study. For example, some emerging frontier research is difficult to be shown in the mapping knowledge domain. The database of this study is limited to the core collection of WoS, and there were no other data sources, such as PubMed and Scopus. It should be noted that Citespace also has its limitations, although these techniques have been used in many bibliometric studies. In summary, the results of the analysis are stable, reliable, and virtually unaffected by subjective experience.

References

[1] N. Fultz and J. Grossklags, "Blue versus red: Towards a model of distributed security attacks," in *International Conference on Financial Cryptography and Data Security*. Springer, 2009, pp. 167–183.

[2] M. Sawyer, "The beginners guide to bitcoin–everything you need to know," *Monetarism—A UK Money and Personal Finance Blog. Retrieved October*, vol. 21, p. 13, 2013.

[3] M. Leising, "The ether thief," https://www.bloomberg.com/features/2017-the-ether-thief/ Accessed August 4, 2021.

[4] J. H. Lee, "Systematic approach to analyzing security and vulnerabilities of blockchain systems," Ph.D. dissertation, Massachusetts Institute of Technology, 2019.

[5] L. Zhu, B. Zheng, M. Shen, S. Yu, F. Gao, H. Li, K. Shi, and K. Gai, "Research on the security of blockchain data: A survey," *arXiv preprint arXiv:1812.02009*, 2018.

[6] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE Symposium on Security and Privacy*. IEEE, 2015, pp. 104–121.

[7] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (sok)," in *International Conference on Principles of Security and Trust*. Springer, 2017, pp. 164–186.

[8] J. M. Merigo, C. A. Cancino, F. Coronado, and D. Urbano, "Academic research in innovation: a country analysis," *Scientometrics*, vol. 108, no. 2, pp. 559–593, 2016.

[9] C. Chen, "Citespace ii: Detecting and visualizing emerging trends and transient patterns in scientific literature," *Journal of the American Society for information Science and Technology*, vol. 57, no. 3, pp. 359–377, 2006.

[10] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *International Conference on Financial Cryptography and Data Security*. Springer, 2014, pp. 436–454.

[11] U. Bodkhe and S. Tanwar, "Taxonomy of secure data dissemination techniques for iot environment," *IET Software*, vol. 14, no. 6, pp. 563–571, 2020.

[12] D. He, G. Hancke, A. Castiglione, and W. Meng, "Introduction to the special section on blockchain techniques for the internet of vehicles security," *Computers and Electrical Engineering*, vol. 87, p. 106860, 2020.

[13] T. Alladi, V. Chamola, R. M. Parizi, and K. K. R. Choo, "Blockchain applications for industry 4.0 and industrial iot: A review," *IEEE Access*, vol. 7, pp. 176 935–176 951, 2019.

[14] Q. Xia, E. B. Sifah, K. O. B. O. Agyekum, H. Xia, K. N. Acheampong, A. Smahi, J. Gao, X. Du, and M. Guizani, "Secured fine-grained selective access to outsourced cloud data in iot environments," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10 749–10 762, 2019.

[15] F. Li, Z. Liu, T. Li, H. Ju, H. Wang, and H. Zhou, "Privacy-aware pki model with strong forward security," *International Journal of Intelligent Systems*, 2020.

[16] C. Song, H. Wang, W. Zhang, S. Sudirman, and H. Zhu, "A blockchain based buyer-seller watermark protocol with trustless third party," *Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering)*, vol. 13, no. 6, pp. 942–950, 2020.

[17] S. Khan, Z. Zhang, L. Zhu, M. A. Rahim, S. Ahmad, and R. Chen, "Scm: Secure and accountable tls certificate management," *International Journal of Communication Systems*, vol. 33, no. 15, p. e4503, 2020.

[18] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K. K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, 2018.

[19] M. Banerjee, J. Lee, and K. K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, 2018.

[20] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Computers & Security*, p. 101966, 2020.

[21] F. Zafar, A. Khan, A. Anjum, C. Maple, and M. A. Shah, "Location proof systems for smart internet of things: Requirements, taxonomy, and comparative analysis," *Electronics*, vol. 9, no. 11, p. 1776, 2020.

[22] S. Guo, Y. Qi, P. Yu, S. Xu, and F. Qi, "When network operation meets blockchain: An artificial-intelligence-driven customization service for trusted virtual resources of iot," *IEEE Network*, vol. 34, no. 5, pp. 46–53, 2020.

[23] L. Feng, H. Zhang, W. T. Tsai, and S. Sun, "System architecture for high-performance permissioned blockchains," *Frontiers of Computer Science*, vol. 13, no. 6, pp. 1151–1165, 2019.

[24] X. Dong, F. Wu, A. Faree, D. Guo, Y. Shen, and J. Ma, "Selfholding: A combined attack model using selfish mining with block withholding attack," *Computers & Security*, vol. 87, p. 101584, 2019.

[25] P. S. Faye, "Use of blockchain technology in agribusiness: Transparency and monitoring in agricultural trade," in *2017 International Conference on Management Science and Management Innovation (MSMI 2017)*, 2017, pp. 38–40.

[26] H. Liang, J. Wu, S. Mumtaz, J. Li, X. Lin, and M. Wen, "Mbid: Micro-blockchain-based geographical dynamic intrusion detection for v2x," *IEEE Communications Magazine*, vol. 57, no. 10, pp. 77–83, 2019.

[27] A. Jindal, G. S. Aujla, N. Kumar, and M. Villari, "Guardian: Blockchain-based secure demand response management in smart grid system," *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 613–624, 2019.

[28] G. Bansal, A. Dua, G. S. Aujla, M. Singh, and N. Kumar, "Smartchain: A smart and scalable blockchain consortium for smart grid systems," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2019, pp. 1–6.

[29] H. Small, "Co-citation in the scientific literature: A new measure of the relationship between two documents," *Journal of the American Society for Information Science*, vol. 24, no. 4, pp. 265–269, 1973.

[30] M. Swan, *Blockchain: Blueprint for a new economy*. O'Reilly Media Inc, 2015.

[31] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2016, pp. 839–858.

[32] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *2016 2nd International Conference on Open and Big Data (OBD)*. IEEE, 2016, pp. 25–30.

[33] M. Salem, M. Mohammed, and A. Rodan, "Security approach for in-vehicle networking using blockchain technology," in *International Conference on Emerging Internetworking, Data & Web Technologies*. Springer, 2019, pp. 504–515.

[34] M. Laxmaiah and T. Neha, "A novel approach for digital online payment system," in *International Conference on Communications and Cyber Physical Engineering 2018*. Springer, 2018, pp. 703–712.

[35] E. Bonnah and J. Shiguang, "Decchain: A decentralized security approach in edge computing based on blockchain," *Future Generation Computer Systems*, vol. 113, pp. 363–379, 2020.

[36] J. Moubarak, M. Chamoun, and E. Filiol, "On distributed ledgers security and illegal uses," *Future Generation Computer Systems*, vol. 113, pp. 183–195, 2020.

[37] X. Yang, X. Yi, S. Nepal, A. Kelarev, and F. Han, "Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities," *Future Generation Computer Systems*, vol. 112, pp. 859–874, 2020.

[38] S. Zhang and J. H. Lee, "Smart contract-based secure model for miner registration and block validation," *IEEE Access*, vol. 7, pp. 132 087–132 094, 2019.

[39] T. A. Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, "A comparative analysis of blockchain architecture and its applications: Problems and recommendations," *IEEE Access*, vol. 7, pp. 176 838–176 869, 2019.

[40] M. Debe, K. Salah, M. H. U. Rehman, and D. Svetinovic, "Iot public fog nodes reputation system: A decentralized solution using ethereum blockchain," *IEEE Access*, vol. 7, pp. 178 082–178 093, 2019.

[41] R. K. Perrons and T. Cosby, "Applying blockchain in the geoenergy domain: The road to interoperability and standards," *Applied Energy*, vol. 262, p. 114545, 2020.

[42] M. Foti and M. Vavalis, "Blockchain based uniform price double auctions for energy markets," *Applied Energy*, vol. 254, p. 113604, 2019.

[43] Y. Li and B. Hu, "An iterative two-layer optimization charging and discharging trading scheme for electric vehicle using consortium blockchain," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2627–2637, 2019.

[44] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3162–3173, 2018.

[45] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*. IEEE, 2015, pp. 180–184.

[46] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*. IEEE, 2017, pp. 557–564.

[47] G. Wood, "A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.

[48] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018.

[49] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[50] A. Saxena, J. Misra, and A. Dhar, "Increasing anonymity in bitcoin," in *International Conference on Financial Cryptography and Data Security*. Springer, 2014, pp. 122–139.

[51] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A scalable blockchain protocol," in *13th USENIX Symposium on Networked Systems Design and Implementation*, 2016, pp. 45–59.

[52] G. Karame, "On the security and scalability of bitcoin's blockchain," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 1861–1862.

[53] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A novel blockchain-based product ownership management system (poms) for anti-counterfeits in the post supply chain," *IEEE Access*, vol. 5, pp. 17 465–17 477, 2017.

[54] D. Tse, B. Zhang, Y. Yang, C. Cheng, and H. Mu, "Blockchain application in food supply information security," in *2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, 2017, pp. 1357–1361.

[55] L. Luu, D.-h. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 254–269.

[56] K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier, and N. Kobeissi, "Formal verification of smart contracts: Short paper," in *Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security*, 2016, pp. 91–96.

[57] H. Liu, C. Liu, W. Zhao, Y. Jiang, and J. Sun, "S-gram: Towards semantic-aware security auditing for ethereum smart contracts," in *2018 33rd IEEE/ACM International Conference on Automated Software Engineering (ASE)*. IEEE, 2018, pp. 814–819.

[58] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable Cities and Society*, vol. 39, pp. 283–297, 2018.

[59] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8770–8781, 2019.

[60] K. Li, H. Li, H. Hou, K. Li, and Y. Chen, "Proof of vote: A high-performance consensus protocol based on vote mechanism amp; consortium blockchain," in *2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE, 2017, pp. 466–473.

[61] X. Xian, Y. Zhou, Y. Guo, Z. Yang, and W. Liu, "Improved consensus mechanisms against censorship attacks," in *2019 IEEE International Conference on Industrial Cyber Physical Systems*. IEEE, 2019, pp. 718–723.

[62] M. Oliveira, L. Reis, D. Medeiros, R. C. Carrano, and D. Mattos, "Blockchain reputation-based consensus: A scalable and resilient mechanism for distributed mistrusting applications," *Computer Networks*, vol. 179, p. 107367, 2020.

[63] J. Bou Abdo, R. El Sibai, and J. Demerjian, "Permissionless proof-of-reputation-x: A hybrid reputation-based consensus algorithm for permissionless blockchains," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, p. e4148, 2021.

[64] R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A user authentication scheme of iot devices using blockchain-enabled fog nodes," in *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications*. IEEE, 2018, pp. 1–8.

[65] S. Tuli, R. Mahmud, S. Tuli, and R. Buyya, "Fogbus: A blockchain-based lightweight framework for edge and fog computing," *Journal of Systems and Software*, vol. 154, pp. 22–36, 2019.

[66] Y. H. Ho, Z. Cheng, P. M. F. Ho, and H. C. Chan, "Mobile intercloud system with blockchain," in *Proceedings of the International MultiConference of Engineers and Computer Scientists*, vol. 1, 2018.

[67] S. M. Toapanta, O. A. Escalante Quimis, L. E. M. Gallegos, and M. R. Maciel Arellano, "Analysis for the evaluation and security management of a database in a public organization to mitigate cyber attacks," *IEEE Access*, vol. 8, pp. 169 367–169 384, 2020.

[68] Y. Raban and A. Hauptman, "Foresight of cyber security threat drivers and affecting technologies," *Foresight*, vol. 20, no. 4, pp. 353–363, 2018.

[69] A. Farion, O. Dluhopolskyi, S. Banakh, N. Moskaliuk, M. Farion, and Y. Ivashuk, "Using blockchain technology for boost cyber security," in *2019 9th International Conference on Advanced Computer Information Technologies*. IEEE, 2019, pp. 452–455.

[70] C. E. Ngubo, P. J. Mcburney, and M. Dohler, "Blockchain, iot and sidechains," in *Proceedings of the International MultiConference of Engineers and Computer Scientists*, Mar. 2019.

[71] S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in *2017 19th International Conference on Advanced Communication Technology*. IEEE, 2017, pp. 464–467.

[72] P. K. Sharma, M. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for iot," *IEEE Access*, vol. 6, pp. 115–124, 2017.

[73] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154–3164, 2017.

[74] P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-vn: A distributed blockchain based vehicular network architecture in smart city," *Journal of Information Processing Systems*, vol. 13, no. 1, pp. 184–195.

[75] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2018.

Ke Yuan is currently an Associate Professor in Henan University of China. He received the Ph.D. degree from Nankai University in 2014. His current interests include applied cryptography, cloud security, and blockchain security.

Yingjie Yan is currently a postgraduate student in Henan University of China. His current interests include applied cryptography and blockchain security.

Lin Shen is currently an undergraduate student in Henan University of China. Her current interest is big data analysis and processing.

Qian Tang is currently an Associate Professor in Henan University of China. She received the Ph.D. degree from Yokohama National University in 2010. Her current research interests include urban ecology, big data analysis and processing, and machine learning.

Chunfu Jia is currently a Professor in Nankai University of China. He received the Ph.D. degree from Nankai University in 1996. His current interests include applied cryptography, computer system security, network security, trusted computing, and malicious code analysis.