sustainability

MDPI

Review

A Quantitative and Qualitative Review of Blockchain Research from 2015 to 2021

Xiaolin Li [1,*], Hongbo Jiao [1], Liming Cheng [1], Yilin Yin [2], Huimin Li [1], Wenqing Mu [3] and Ruirui Zhang [3]

[1] Department of Construction Engineering and Management, North China University of Water Resources and Electric Power, Zhengzhou 450046, China
[2] School of Management, Tianjin University of Technology, Tianjin 300384, China
[3] The First Institute of Resources and Environment Investigation of Henan Province, Zhengzhou 450000, China
* Correspondence: lixiaolin@ncwu.edu.cn

Abstract: Blockchain has the potential to reconfigure the contemporary economic, legal, political and cultural landscape, causing a flood of research on this topic. However, limited efforts have been made to conduct retrospective research to appraise the blockchain studies in the recent period, easily leading to a neglect of new technological trends. Consequently, the present research designs a quantitative- and qualitative-analysis procedure to review the latest research status. Adopting a four-step workflow, six research hotspots (i.e., the specific application areas of blockchain technology, the integration of blockchain and other technologies, the driving factors of blockchain, the values of blockchain technology, the types of blockchain and the core technologies of blockchain) and five research frontiers (i.e., entrepreneurship, contract, industrial internet, data management and distributed ledger technology) were detected using quantitative analysis. Furthermore, three other topics (i.e., the Internet of things, access control and trust) and two research gaps (i.e., the true effect of blockchain technology on firms' operational efficiency and the regulation of the "dark sides" of blockchain technology) were also identified, using qualitative analysis. Finally, the evolutionary paths were qualitatively analyzed, and then three phases of blockchain research were summarized. The conclusions are able to provide a more comprehensive enlightenment regarding blockchain's research hotspots, research frontiers, evolutionary paths and research gaps in the recent period, from 2015 to 2021, and to provide a reference for future research.

Keywords: blockchain; cryptography; smart contract; distributed storage; consensus mechanism; visualized analysis

Citation: Li, X.; Jiao, H.; Cheng, L.; Yin, Y.; Li, H.; Mu, W.; Zhang, R. A Quantitative and Qualitative Review of Blockchain Research from 2015 to 2021. *Sustainability* **2023**, *15*, 5067. https://doi.org/10.3390/su15065067

Academic Editor: Fabrizio D'Ascenzo

Received: 16 February 2023
Revised: 3 March 2023
Accepted: 9 March 2023
Published: 13 March 2023

1. Introduction

Blockchain was first proposed by Nakamoto, and was adopted as a system for electronic transactions without relying on trust [1]. The core technologies of blockchain include cryptography, distributed storage, consensus mechanism and smart contract. Cryptography, as the cornerstone of blockchain, endows blockchain with the characteristics of being tamper-proof and collision-proof, ensuring the security of the whole blockchain system [2]. As the framework of blockchain, distributed storage uses distributed ledger to store data and endows blockchain with characteristics of decentralization, which can effectively solve problems such as data loss [3]. Although distributed ledgers can guarantee the safe operation of data, it usually faces the Byzantine generals problem. Consensus mechanism, as a new technology to solve the Byzantine generals problem, coordinates the accounts of all nodes in blockchain networks and then maintains the normal operation of the whole blockchain [4]. In addition, the emergence of blockchain makes it possible to apply smart contracts on a large scale. Smart contracts, with the advantages of disintermediation, transparency and public trust, build the transactional relationship of contracts into a technical code that is executed automatically [5] and broadens the application scenarios of blockchain technology [6]. The above four core technologies make blockchain decentralized, trustless,

open and data-reliable [7] (Skowroński, 2019), which attracts much attention from scholars. Additionally, as a cryptographic-based distributed ledger [8], blockchain can facilitates peer-to-peer value transfers of all sorts, from digital currency to physical commodities and land titles, without the need for an intermediary such as banks, accountants, or lawyers [5]. What is more, blockchain technology can keep an open record of all transactions or computerized events that have been executed and shared among partaking parties [9]. In other words, blockchain is a distributed database capable of providing an unalterable record of digital transactions [10]. As Wang et al. [11] pointed out, the blockchain network has the characteristics of decentralization and transparency, so that the information shared among traders in real time cannot be tampered with, which meets the requirements of the digital age [12]. These features contribute to its extensive applications in various domains, such as insurance [13,14], finance [15,16], supply chain [17,18], healthcare [19], construction industry [20] and fraud detection [21].

Given its popularity, scholars have published several systematic reviews of blockchain research in various fields. For example, Hölbl et al. [22] conducted a systematic review of the adoption of blockchain platforms in health care. Additionally, Bodkhe et al. [23] conducted a systematic review of various solutions based on blockchain from a technical perspective, focusing on topics such as data storage, network latency, auditability, immutability and traceability. This research provided insights to readers of the importance of blockchain technology for various smart applications. In addition, many scholars have conducted application scenario analyses and reviews on blockchain research for the purpose of better understanding the research progress of this field. For instance, Kim [24] analyzed the blockchain development status based on examining the relationship between blockchain patents and enterprise value. Zheng et al. [25] summarized the blockchain framework, and typical consensus algorithms are compared in different application scenarios and phases. Moreover, they listed current challenges and future development trends of blockchain technology. Based on data gathered from the Web of Science (WoS) database, Guo [26] conducted a visual analysis on blockchain research including its research status and trends by using Citespace software. However, blockchain technology is developing with each new day, and new research on blockchain is deepening, with a batch of new research hotspots and frontiers emerging. All of these make current reviews unable to keep pace with today's blockchain technology, easily causing a neglect in new technological trends. Therefore, it is necessary to analyze the development status and trends of blockchain by considering the new literature. This study aims to fill this gap and pick up where the current researches left off. For this purpose, the present research intends to use quantitative analysis (i.e., scientometric analysis) and qualitative analysis (i.e., content analysis) to review blockchain research in the most recent period, from 2015 to 2021. As exhibited in Figure 1, by designing and adopting a four-step research procedure which is composed of data collection, descriptive analysis, quantitative analysis, and qualitative analysis to supplement conclusions form quantitative analysis, this research can achieve the following research objectives: (1) to analyze the main research hotspots in the blockchain research field; (2) to identify the current research frontiers for deeper research; (3) to describe the research evolutionary trends; and (4) to grasp the research gaps which will guide future research directions. The conclusions can enlighten researchers more comprehensively as to blockchain's research hotspots, research frontiers, evolution paths and research gaps in the more recent period, from 2015 to 2021, and provide reference for future research.

The remaining structure of this paper is summarized as follows. Section 2 proposes a research design combining quantitative with qualitative analysis and explains the process of data collection in detail. The descriptive analysis, quantitative analysis and qualitative analysis are presented in Section 3. Through this design, this research identified the research hotspots, frontiers, evolution paths and research gaps of blockchain research from 2015 to 2021. This research concludes with an overview, limitations and recommendations in Section 4.

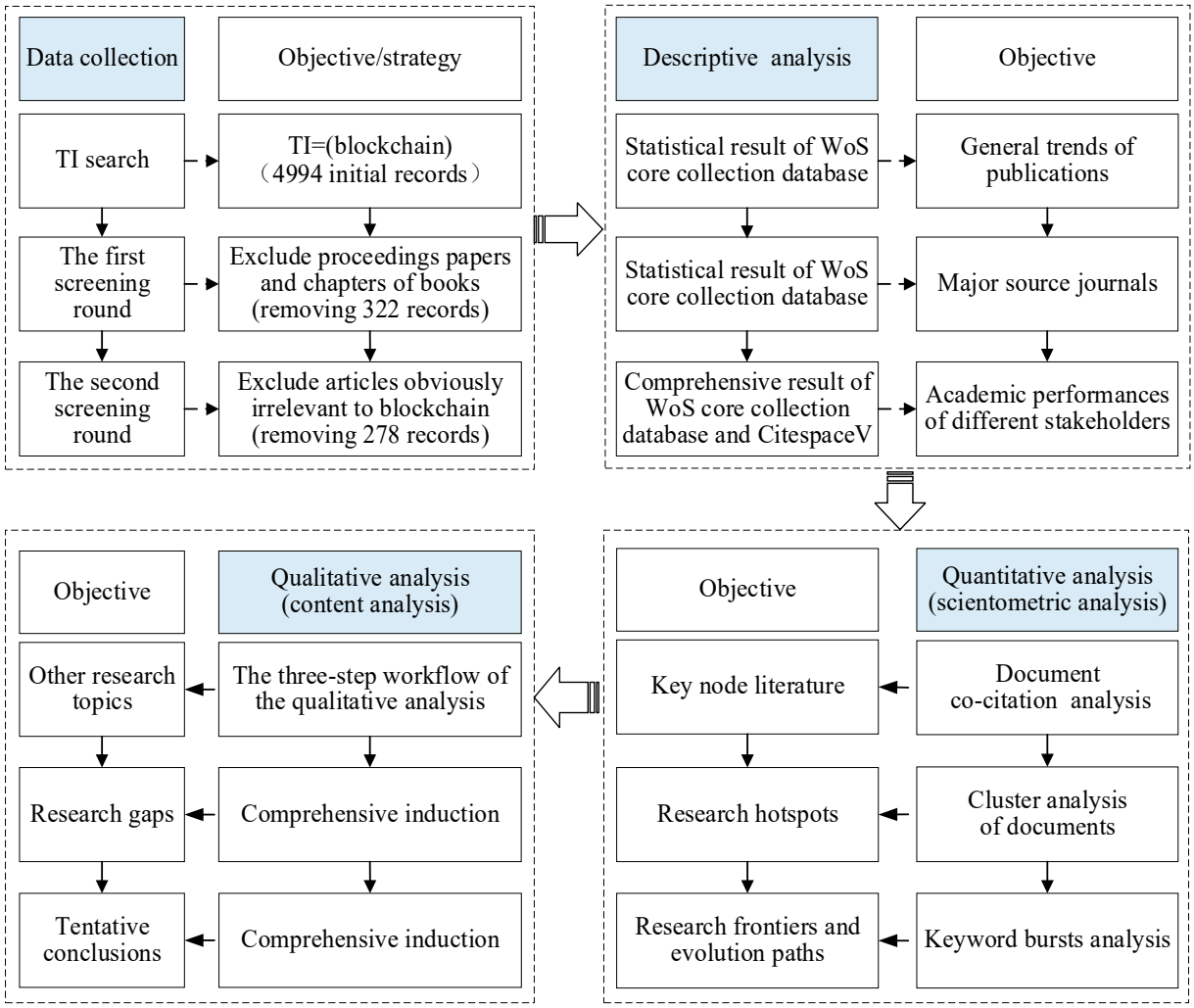

Figure 1. The research procedure of the present study.

2. Research Design

2.1. Methods

In this study, quantitative and qualitative analysis were adopted to review blockchain research. By means of CitespaceV, research hotspots and frontiers can be preliminarily described using quantitative analysis, objectively. By quantitative analysis complementing the results of quantitative analysis, some important but neglected research topics can be identified.

As noted above, CitespaceV is the main tool used for quantitative analysis in this study. By collecting literature data from the WoS database, visualized clusters of co-cited references can be generated by CitespaceV [27]. These visualized clusters are usually regarded as research hotspots in research communities [28,29]. In comparison with other bibliometrics software, CitespaceV has its own special advantage, that is, it can conduct keyword-burst analysis. Specifically, a keyword which has been of highly concern to the academic community in a certain period of time will be marked as citation burst [30]. So, this function is usually utilized to find research frontiers. Consequently, this study mainly conducts document co-citation analysis and keyword-burst analysis, adopting CitespaceV to identify the research hotspots and research frontiers of blockchain research. To better complete document co-citation analysis, citation frequency (CF), betweenness centrality (BC) and citation burst (CB) are constructed to define whether the literatures are important or not. CF stands for the recognition of literature by researchers, which is a sign for measuring the academic contribution of a publication [30]. As far as BC is

concerned, an article with a higher BC (>0.1) will act as a medium among different groups. As Chen et al. [27] pointed out, the high-CB article means that it attracts a wide range of scholars in a certain period of time. Moreover, the cited references are selected as the nodes in this study, and the importance of nodes (N_{IF}) is judged by N_{CF} (nodes' CF) and N_{BC} (nodes' BC), that is, $N_{IF} = N_{CF} \times (N_{BC} + 1)$. In addition, citation bursts of keywords indicate the speed with which new keywords are taken up [31]. Therefore, keyword-burst analysis is served as the method to detect new trends and frontiers of the blockchain research field.

With regard to qualitative analysis, relevant experts have pointed that that bibliometric analysis can never act as a substitute for manual reviews, despite the fact that bibliometric analysis can objectively and fairly reveal the relationship between different studies [32]. Therefore, in-depth qualitative analysis must inevitably be carried out to supplement the conclusions drawn from quantitative analysis and identify the important research topics neglected by quantitative analysis due to low co-citation frequency, as well as to find out research gaps.

2.2. Data Collection and Processing

The *WoS* database is one of the largest and most prestigious citation databases in the world, and contains many authoritative and influential international academic journals and publications [28,29]. What is more, it is often used as a data source to carry out bibliometric analysis in many research fields [28,29,33–35]. Therefore, we took the WoS database as the main source to collect relevant literature on blockchain research. Important information from publications, such as publication year, source journals, etc., was gathered. In addition, we set the time span from 2015 to 2021, for the reason that blockchain technology has been attracting attention from various government agencies since 2015, and research around blockchain in various countries increased greatly in 2015 [36]. Furthermore, the present research intends to track the latest development of blockchain research, so the end date was set for 31 December 2021.

Specifically, we entered the following search codes in the WoS database for literature screening: TI = (blockchain). Here, the "TI" indicates the title of the publication, while "()" means the exact search. In this way, we can obtain accurate results related to blockchain research. In addition, as illustrated in the Figure 1, we designed a two-round literature screening process. First of all, we excluded proceedings papers and chapters of books which could not provide enough valuable information when compared with journal articles. Secondly, journal articles that were obviously unrelated to the blockchain research field were also screened out. Therefore, the data accuracy of this study is guaranteed by eliminating publications that are not in the scope of or do not focus on blockchain research. Specifically, the title-based search in the WoS database obtained 4994 relevant initial records. The first round of screening removed 322 records, such as Pankova [37], because they did not provide as much information as journal papers. In addition, the second round of screening excluded 278 records, such as Serra-Navarro et al. [38], which focused on problems from other subject areas (i.e., art). Moreover, it was essential to carry out a quantitative analysis based on the function of removing duplicate document records from CitespaceV, resulting in 65 duplicate literature records being deleted. As a result, 4329 final records were gathered in this study.

3. Quantitative and Qualitative Analysis

3.1. Descriptive Analysis

3.1.1. The Overall Trends of Publications

Figure 2 shows the distribution of 4329 records in 2015–2021. As can be seen in Figure 2, the number of articles published has surged since 2015. This shows that the research community has become more and more interested in the output of blockchain research in recent years.

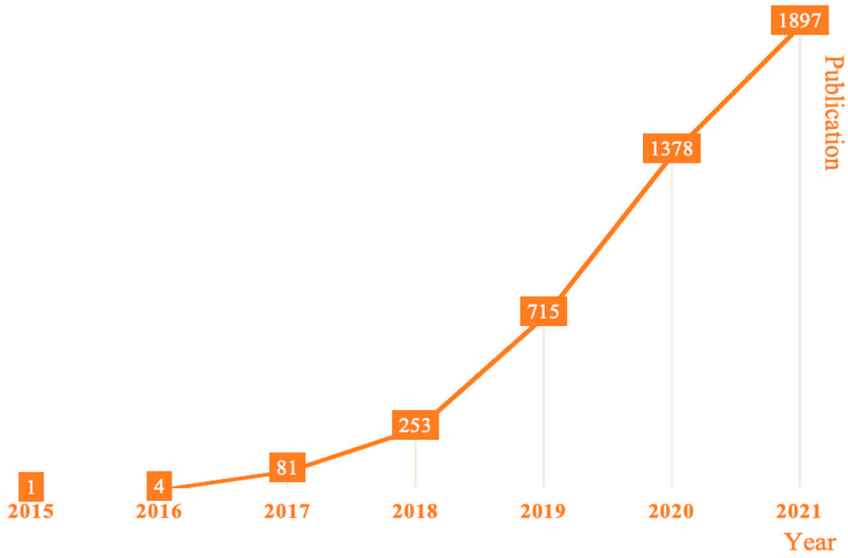

Figure 2. Publications of blockchain research from 2015 to 2021.

3.1.2. Primary-Source Journals

This research identifies and evaluates selected primary-source journals for journal articles on blockchain research. The results are presented in Table 1.

Table 1. The top10 source journals in the blockchain research field from 2015 to 2021.

Source Journal	Publication	Co	Countries	Field
IEEE Access	531 (12.79%)	2405	USA	CS
IEEE Internet of Things Journal	166 (3.83%)	1392	USA	CS
Sensors	143 (3.30%)	746	Switzerland	EN
Sustainability	131 (3.03%)	457	Switzerland	S&T
Applied Sciences-Basel	106 (2.45%)	288	Switzerland	EN
IEEE Network	91 (2.10%)	620	USA	CS
Electronics	81 (1.87%)	111	Switzerland	CS
Frontiers In Blockchain	79 (1.82%)	416	Germany	BT
Future Generation Computer System	76 (1.76%)	1353	The Netherlands	CS
IEEE Transactions on industrial informatics	75 (1.76%)	1113	USA	CS

Note: Co = frequency of co-citations of journals; Country = host countries; CS = computer science; EN = engineering; S&T = Sustainability science and technology; BT = blockchain technology.

The total 890 journals published 4329 articles from 2015 to 2021, and Table 1 shows the top 10 publishers with the highest yield in the blockchain research field, including journal percentages and co-citation frequencies as assessed by Citespace's journal co-citation function, and journals' host countries and research areas. Obviously, most of the top 10 journals are closely related to computer science. IEEE Access had published 531 articles in the blockchain research field, ranking first. The journal with the second largest number of publications is IEEE Internet of Things Journal (publication = 166), followed by *Sensors* (publication = 43). According to Li et al. [29], the degree of authority and influence of a journal can be evaluated by its citation frequency. Thus, from this perspective, the top three most influential journals were IEEE Access (co-citation = 2405), IEEE Internet of Things Journal (co-citation = 1392) and Future Generation Computer System (co-citation = 1353). Considering the publishing quantity and frequency of co-citations of journals, this research takes IEEE Access and the IEEE Internet of Things Journal as the most influential journals in the blockchain research field. In addition, it

is worth noting that Sensors, Sustainability, Applied Sciences-Basel and Electronics are all MDPI journals. Moreover, other MDPI journals such as Mathematics and Journal of Theoretical and Applied Electronic Commerce Research have also published a large number of valuable articles in the blockchain research field. Indeed, MDPI publisher has published 2235 articles focusing on blockchain technology until now, making a great contribution to the advancement of this research field.

3.1.3. Academic Performance of Different Stakeholders

The academic contribution of stakeholders was separated into different levels: macro level (countries/regions), intermediate level (institutions) and micro level (authors). Such classification can provide researchers with a comprehensive understanding of the scholarly performances of important stakeholders at all levels [29,39]. In summary, authors from 111 countries/regions published their articles in the blockchain research field from 2015 to 2021. Table 2 presents the top10 most effective countries/regions. It can be seen that China exceeds the number of papers published by all other countries/regions, with 1641 papers. It is obvious that the top three countries, including China, the United States, and India published 64.33% of all the publications, showing their huge contributions. Among other countries/regions, researchers from South Korea, Great Britain, Australia, Canada, Saudi Arabia, Taiwan, and Italy, contributed greatly to this field, as well. Because blockchain has huge application prospects, many countries/regions have introduced a series of policies to encourage the development and application of blockchain technology. For instance, China listed blockchain technology as a strategic frontier technology, requiring an advanced layout for the first time in the 13th Five-Year National Informatization Plan in 2016. Therefore, this year is also the first year for Chinese scholars to conduct blockchain research (He et al., 2018). Although blockchain-related research started late in China, the Chinese government attaches great importance to the advancement of blockchain technology. For instance, in March 2021, the Global Energy Interconnection Development and Cooperation Organization (GEIDCO) put forward a plan to achieve carbon reduction targets by building the Chinese energy internet and using blockchain technology. That is why blockchain technology is so popular in China, and the number of research studies is growing rapidly. In addition, the connection between different countries and regions of the academic activities of central countries/regions are identified, using betweenness centrality (>0.1). To be specific, England (centrality = 0.16), Saudi Arabia (centrality = 0.14) and USA (centrality = 0.13) occupy the key position in connecting different countries and regions, showing their outstanding academic performances in the blockchain research field (as can be seen in Table 2).

Table 2. The top10 productive countries/regions in the blockchain research field from 2015 to 2021.

Country/Region	Publication	Centrality	Country/Region	Publication	Centrality
China	1641 (37.91%)	0.06	Australia	279 (6.44%)	0.06
USA	756 (17.46%)	0.13	Canada	259 (5.98%)	0.10
India	388 (8.96%)	0.08	Saudi Arabia	239 (5.52%)	0.14
South Korea	349 (8.06%)	0.03	Taiwan	179 (4.13%)	0.03
England	340 (7.85%)	0.16	Italy	160 (3.70%)	0.08

From an intermediate-level (institution) perspective, Table 3 displays the top 10 institutions in terms of the number of publications. As can be seen, Beijing University of Posts and Telecommunications topped the list with 113 papers, followed by the Chinese Academy of Sciences (publication = 91). The remaining productive organizations came from Saudi Arabia, China, Singapore and the USA.

Table 3. The top10 most productive institutions in the blockchain research field from 2015 to 2021.

Institution	Country	Publication	Percentage	AVE
Beijing University of Posts and Telecommunications	China	113	2.61%	24.79
Chinese Academy of Sciences	China	91	2.10%	16.82
King Saud University	Saudi Arabia	82	1.89%	16.49
Xidian University	China	77	1.78%	16.01
University of Electronic Science and Technology of China	China	72	1.66%	30.46
Beijing Institute of Technology	China	53	1.22%	23.77
Wuhan University	China	52	1.20%	17.18
Nanyang Technological University	Singapore	51	1.18%	34.83
University of Texas at SAN Antonio	USA	51	1.18%	31.82
Asia University, Taiwan	China	49	1.13%	13.16

Note: AVE = the average citation frequency of all papers in the corresponding institutions.

Additionally, AVE in Table 3 refers to the average citation frequency of an institutions' correlative publications, as AVE = N_{CF} /n. Here, "N_{CF}" represents the citation frequency of all publications of institutions, and "n" means the number of papers published by different institutions. Consequently, AVE could be used to describe the academic influence and visibility of institutions (Li et al., 2021). It is noteworthy that the AVE of Nanyang Technological University (AVE = 34.83) and University of Texas at SAN Antonio (AVE = 31.82) are quite high, indicating that these institutions have great academic influence and popularity.

Table 4 lists the top10 most productive authors in the field of blockchain research. It can be seen that all the listed scholars have at least 26 articles in the blockchain research field. To further evaluate their academic performances, we used both h-index and average citation per publication (AVE). In this respect, Yan Zhang had the highest h-index, of 25. In addition, Yan Zhang and Dusit Niyato had an AVE of 42.43 and 40.79, respectively, showing their outstanding influence in this field. All thing considered, this research takes Yan Zhang, Kim-Kwang Raymond Choo and Neeraj Kumar as the core authors in the blockchain research field.

Table 4. The top10 productive authors in the blockchain research field from 2002 to 2020.

Author	Publi-	h-Index	AVE	Author	Publi-	h-Index	AVE
Neeraj Kumar	49	22	21.84	F. Richard Yu	30	16	28.76
Khaled Salah	47	15	29	Sudeep Tanwar	28	12	15.33
Kim-Kwang Raymond Choo	45	24	33.91	Mohsen Guizani	28	14	31.61
Yan Zhang	31	25	42.43	Debiao He	28	15	29.07
Raja Jayaraman	31	8	8.14	Dusit Niyato	26	16	40.79

Note: Publi- = Publication; AVE = average citations per publication.

3.2. Quantitative Analysis

3.2.1. Document Co-citation Analysis

As mentioned previously, we utilized CitespaceV to conduct a literature co-citation analysis, and evaluated the importance degree (N_{IF}) of the literature from 2015 to 2021, based on the formula of $N_{IF} = N_{CF} \times (N_{BC} + 1)$, similar to Sun and Zhai [40]. Table 5 presents the top 10 key publications' specific N_{IF} data, which range from 519.12 to 205.02. To be specific, Christidis and Devetsikiotis [41], Zheng et al. [25], and Zheng et al. [42] received an NIF of 519.12, 380.77 and 318.15, respectively, ranking within the top three.

Table 5. The top 10 key documents in the blockchain research field from 2015 to 2021.

Literature	Journal	Topic	N_{CF}	N_{BC}	N_{IF}
Christidis and Devetsikiotis (2016) [41]	IEEE Access	A	504	0.03	519.12
Zheng et al. (2017) [25]	IEEE International congress on Big Data	B	377	0.01	380.77
Zheng et al. (2018) [42]	International Journal of Web and Grid Services	A	315	0.01	318.15
Zyskind et al. (2015) [43]	IEEE Security and Privacy Workshops	C	284	0.01	286.84
Androulaki et al. (2018) [44]	Proceedings of the Thirteenth Eurosys Conference	A	281	0.02	286.62
Kosba et al. (2016) [45]	IEEE Symposium on Security and Privacy	A	235	0.03	242.05
Azaria et al. (2016) [46]	International Conference on Open and Big Data	A	214	0.05	224.70
Saberi et al. (2019) [47]	International Journal of Production Research	A	214	0.02	218.28
Aitzhan et al. (2016) [48]	IEEE Transactions on Dependable and Secure Computing	C	204	0.06	216.24
Yli-Huumo et al. (2016) [49]	Plos One	B	201	0.02	205.02

Notes: A = The application of blockchain technology; B = Literature review; C = Blockchain privacy protection.

In addition, through the research subjects of the top 10 key-node articles, it is obvious that these articles mainly focus on the application of blockchain technology (i.e., topic A).

Subsequently, cluster analysis was adopted after document co-citation analysis. In Figure 3, clustering labeled with the LLR algorithm visually presents the main research topics of blockchain research. The correlative parameters of the network are labeled in Figure 3. In particular, the modularity, Q, of 0.8146, is fairly high (>0.7), which demonstrates that inter-cluster connections are considerable and overwhelming [50]. In addition, the mean silhouette utilized to evaluate the average homogeneity of the network is 0.7414 (>0.5), showing an ideal silhouette value and a more uniform structure [50].

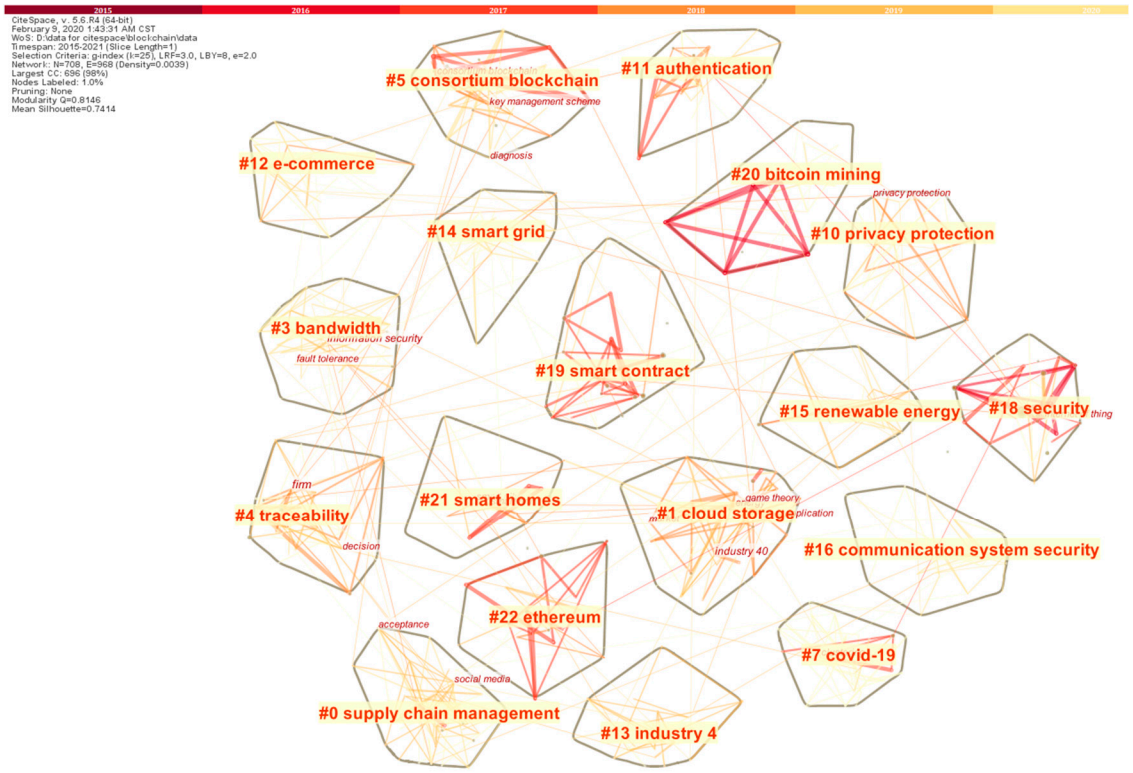

Figure 3. Literature cluster analysis in blockchain research field.

It is worth noting that we set the parameter of *Look Back Years* to seven (the initial value from the software) in *CitespaceV*. Therefore, four clusters include the literature published before 2015. To keep in line with the research objectives, this research removed the clusters including much of the literature published before 2015 (such as cluster #2) in the follow-up

analysis, because this research aimed to track the latest research progress in blockchain research from 2015 to 2021. In addition, in Figure 3, clusters with a small number of members are also ignored. In this way, we finally achieve 18 effective clusters, as seen in Table 6.

Table 6. Cluster of co-references for blockchain research from 2015 to 2021.

Cluster	Cluster Label (LLR)	Size	Silhouette	Representative Article
#0	supply chain management	46	0.96	Khanna et al. (2020) [51]; Saberi et al. (2020) [52]
#1	cloud storage	44	0.934	Miao et al. (2020) [53]; Sharma et al. (2020) [54]
#3	bandwidth	38	0.882	Zhang et al. (2020) [55]
#4	traceability	38	0.906	Guo et al. (2021) [26]; Mitani and Otsuka (2020) [56]
#5	consortium blockchain	37	0.968	Guo et al. (2020) [57]
#7	COVID-19	32	0.977	Tan et al. (2020) [58]; Kalla et al. (2020) [59]
#10	privacy protection	29	0.868	Patil et al. (2020) [60]; Sun et al. (2021) [30]
#11	authentication	28	0.98	Mwitende et al. (2020) [61]; Cui et al. (2020) [62]
#12	e-commerce	28	0.95	Deng et al. (2021) [63]; Harish et al. (2021) [64]
#13	industry 4	28	0.789	Zuo et al. (2021) [65]; Aste et al. (2017) [66]
#14	smart grid	28	0.929	Tanwar et al. (2020) [67]; Mengelkamp et al. (2018) [68]
#15	renewable energy	27	0.856	Huh et al. (2019) [69]; Tsao and Thanh (2021) [70]
#16	communication system security	26	0.876	Gao et al. (2021) [71]
#18	security	24	0.988	Lin and Liao (2017) [72]
#19	smart contract	23	1	Ciatto et al. (2020) [73]; Macrinici et al. (2018) [74]
#20	bitcoin mining	22	0.849	Kufeoglu and Zkuran (2019) [75]
#21	smart homes	18	0.93	Sabir et al. (2020) [52]; Hosseinian et al. (2020) [76]
#22	ethereum	17	0.966	Tikhomirov et al. (2017) [77]

The clusters are sorted by size. Table 6 shows that cluster 0, "supply chain management", is the largest cluster, with 46 literature articles, followed by cluster 1, "cloud storage", with 44 members and cluster 3, "bandwidth", with 38 members. Additionally, the silhouettes utilized to assess clusters' homogeneity are showed, and the representative documents of these cluster are chosen for the reason of their high co-citations. Therefore, the representative documents are worthy of more attention.

Cluster 0, "supply chain management", has 46 members. This cluster reflects hotspot 1: the specific application areas of blockchain technology. In addition, cluster 7 (COVID-19), cluster 12 (e-commerce), cluster 13 (industry 4), cluster 14 (smart grid), cluster 15 (renewable energy), cluster 20 (bitcoin mining) and cluster 21 (smart homes) also represent the application scenarios of blockchain technology. With the globalization of supply chains, the management of supply chains becomes more and more difficult and complex. Correspondingly, there are many potential obstacles and difficulties to overcome when using blockchain technology to promote the sustainable development of supply chains. These barriers and difficulties are multifaceted, and more empirical research is needed to explore the significance of them [52]. However, this does not prevent blockchain from playing an irreplaceable role in many other fields. For instance, blockchain technology can play an important role in healthcare, reducing the spread of misinformation during COVID-19 [78]. Similarly, electronic transactions based on blockchain cryptocurrency systems have become very popular in commerce. As an emerging technology, blockchain can add trust, security and decentralization to different industrial sectors, providing detailed guidance for future Industry 4.0 development as well [79]. As for the bitcoin-mining algorithm, blockchain technology' security relies solely on the computationally intensive bitcoin-mining algorithm, which is an essential part of maintaining the entire blockchain network and can prevent double spending of bitcoins and tampering with confirmed transactions. What is more, this kind of algorithm is not excessive, in contrast to the public perception that bitcoin mining is a serious waste of energy [80]. In addition, blockchain technology can drive innovation in energy. It is well known that the increasing availability of renewable energy in the energy system requires new market approaches to pricing and distribution.

Blockchain could effectively provide a market platform for trading in local energy production without the need for a central intermediary [68]. A smart grid is a new type of electricity that effectively combines green and renewable-energy technologies; this grid is undergoing a transformation, to decentralized topology from its centralized form, during which blockchain technology is needed to solve the major security challenges that smart grids face in this transition [81]. In addition to the above application areas, blockchain can also better serve the public in daily life. The advantages of blockchain, such as privacy, credibility and reliability can be fully reflected in the smart-furniture environment, which can further play an important role in the Internet-of-things industry [82].

Cluster 1, "cloud storage", has 44 members, and it reflects hotspot 2: the integration of blockchain and other technologies. Cloud storage is an emerging storage method derived from the development of cloud computing and it can reduce the burden of local storage [83]. However, traditional cloud storage inevitably brings data integrity and privacy issues. To solve the above problems, Li et al. [84] put forward a blockchain-based distributed cloud-storage security architecture, and verified that the architecture was significantly superior to the traditional architecture in terms of security and network-transmission delay. Although public verification technology can protect data integrity, this method is prone to be affected by the work schedule of auditors. Based on this, Zhang et al. [85] proposed a certificateless public-authentication scheme, CPVPA, using blockchain technology to solve this problem, which can help users check whether auditors can complete their work within the specified time. In their framework, Zhang et al. [85] proved that CPVPA is secure, and does not have certificate management problems.

Cluster 3, "bandwidth", has 38 members, and it reflects hotspot 3: the driving factors of blockchain. Similarly, cluster 11 (authentication) also represent this hotspot. Bandwidth provides the basis for the development of the blockchain 1.0 era represented by bitcoin. To ensure blockchain operational efficiency, network bandwidth fundamentally limits blockchain technology throughput. That is to say, the blockchain network cannot reach consensus and consistency without an appropriate network bandwidth. Therefore, the rational allocation of bandwidth resources can affect the system utility [86]. However, faced with the differences in the parallelism requirements of various new computing tasks, the efficiency needs to be maximized by considering the allocation of computing and bandwidth resources in an integrated manner. For example, a computing task with parallelism differences is introduced in a mobile edge computing system, and a heterogeneous computing framework is needed to properly partition the different computing tasks, to achieve efficient execution of the task [55]. In addition, Ethernet has established a programmable, Turing-complete blockchain program by adding smart contract technology, driving the blockchain technology into the 2.0 era [87]. The core value proposition of Ethereum is a full-featured programming language suitable for implementing complex business logic [77].

Cluster 4 "traceability" has 38 members, and it reflects hotspot 4: the values of blockchain technology; cluster 10 (privacy protection), cluster 11 (authentication), cluster 16 (communication system security) and cluster 18 (security) also reflect this hotspot. As mentioned before, blockchain is a distributed database recording the input and output of every transaction, which makes it easy to track changes in asset and trading activities [10]. In addition, blockchain can improve the entire data-management process in a complex network consisting of processors, retailers, regulators and consumers. Although the decentralization and transparency of blockchain will enable information sharing in real time [11], blockchain technology can still protect identity privacy (referring to the association between user-identity information and blockchain address) and transaction privacy (referring to the transaction records stored in blockchain and the knowledge behind the transaction records) of users. For instance, Wang and Li [88] designed a medical-data privacy-protection system that integrates blockchain, group signature and asymmetric encryption, realizing reliable medical-data sharing among medical institutions, and protecting patients' data privacy. As for authentication, although anonymity is an important topic to highlight in protecting the privacy of users' transactions, the need for proof of identity is an

objective in the development of blockchain. In the Internet of things especially, things are processed and data are exchanged without human intervention. Therefore, these entities need to be identified and verified against each other, otherwise they will become targets for malicious users or malicious use [89]. Nowadays, the Internet of things is developing rapidly, but it is inevitable that there will be many violations of security policies. As a result, the way in which the privacy of the communicating parties can be protected in network communication has attracted more and more attention. Mishra and Bhanodiya [90] conducted a review of cryptography–steganography systems which combine cryptography with steganography, and found that the system provides a high level of security for the exchange of critical information. With the gradual application of blockchain technology, its security is also a concern of scholars. Although blockchain technology has advantages, such as reliable information exchange and complete data storage, there are still many security risks in the blockchain system at this stage. For instance, the system based on blockchain is weak [91]. Since 2009, the bitcoin and Ethernet platforms related to blockchain technology have suffered a loss of USD 86.7 million. Similarly, Zheng et al. [42] pointed out that some self-centered miners will collude to attack blockchain. Therefore, blockchain is not as safe as expected, and many attacks have occurred.

Cluster 5, "consortium blockchain," has 37 members, and it reflects hotspot 5: the types of blockchain. As a kind of blockchain, the consortium blockchain refers to the blockchain technology that can be controlled by pre-selected nodes in the process of consensus [92]. It is well known that there are three types of blockchain, consisting of public blockchain, private blockchain and consortium blockchain. In terms of scale and openness, consortium blockchain is the one between private blockchain and public blockchain. That is to say, the consortium blockchain is partially decentralized, has high throughput, and fast transactions. Therefore, the consortium blockchain is widely considered to be an ideal tool in financial supervision. It can ensure financial transactions are better protected, while the financial sector and regulatory institutions are able to keep track of participants more easily [93]. In addition, well-known applications of consortium blockchain include R3 and Hyperledger, which can support a wide range of scene applications in banking, finance, insurance, medical and other industries. Given the above advantages, consortium blockchain is attracting more and more attention, and is becoming one of the hotspots in the blockchain research field.

Cluster 19, "smart contract", has 23 members, and it reflects hotspot 6: the core technologies of blockchain. As a kind of computer program proposed by Nick Szabo, smart contract is usually used to replicate the actions described in physical/traditional contracts, and its objectives consists of visibility, confirmability, confidentially and performability [94]. Bitcoin and its scripting language indicate that blockchain has laid the foundation for executing smart contracts because of its read-add property [95]. Smart contracts automatically respond to the needs of the main body in real time, greatly improving service efficiency without the participation of third-party central institutions [96]. Moreover, smart contracts can alleviate information asymmetries, and have the potential to expand the contract space and improve consensus quality [6]. In addition, cryptography, distributed storage, and consensus mechanisms are core technologies of blockchain. These four core technologies build a self-running social-trust network that does not rely on third parties, which can then promote the whole society to start valuable interconnections and make a positive contribution to the circular economy [97].

In summary, we detected six research hotspots in the blockchain research field, through quantitative analysis, consisting of the specific application areas of blockchain technology, the integration of blockchain and other technologies, the driving factors of blockchain, the values of blockchain technology, the types of blockchain and the core technologies of blockchain.

3.2.2. Keyword-Burst Analysis

As noted above, keyword-burst analysis was utilized to detect research frontiers and to grasp emerging trends during a certain time. Figure 4 shows the top 20 keywords with the strongest bursts in the blockchain research field from 2015 to 2021.

Top 20 Keywords with the Strongest Citation Bursts

Keywords	Year	Strength	Begin	End	2015 - 2021
bitcoin	2015	20.3359	**2016**	2019	
access control	2015	3.6955	**2016**	2018	
cryptocurrency	2015	8.286	**2017**	2019	
consortium blockchain	2015	2.8172	**2017**	2019	
blockchain	2015	5.9157	**2017**	2017	
key management scheme	2015	3.9814	**2018**	2019	
game theory	2015	3.4523	**2018**	2019	
privacy-preserving	2015	4.4965	**2018**	2019	
identity	2015	3.1169	**2018**	2019	
cloud	2015	5.8639	**2018**	2019	
electricity	2015	3.6366	**2018**	2019	
architecture	2015	8.3345	**2019**	2019	
fairness	2015	3.626	**2019**	2019	
fog computing	2015	2.9767	**2019**	2019	
electronic health record	2015	4.4888	**2019**	2019	
entrepreneurship	2015	2.8703	**2020**	2021	
industrial internet	2015	3.4739	**2020**	2021	
contract	2015	5.8154	**2020**	2021	
data management	2015	2.8703	**2020**	2021	
distributed ledger technology (dlt)	2015	2.8703	**2020**	2021	

Figure 4. Top 20 keywords of blockchain research.

As shown in Figure 4, the three strongest bursts were "bitcoin" (strength = 20.34, 2016–2019), "architecture" (strength = 8.33, 2019–2019) and "cryptocurrency" (strength = 8.29, 2017–2019), and these keywords represent the hotspots of blockchain research in the corresponding periods. In the most recent years, from 2020 to 2021, "entrepreneurship" (strength = 2.87, 2020–2021), "contract" (strength = 5.82, 2020–2021), "industrial internet" (strength = 3.47, 2020–2021), "data management" (strength = 2.87, 2020–2021) and "distributed ledger technology" (strength = 2.87, 2020–2021) are citation breakout points, all of which represents the research frontiers of the blockchain research field in the last few years.

Additionally, based on the results of the keyword-burst analysis, the research evolutionary trends of blockchain can be divided into three stages. In the first research stage (2015–2017), the main research subjects covered bitcoin (the burst strength of bitcoin = 20.34) and cryptocurrency (the burst strength of cryptocurrency = 8.29). As stated before, bitcoin uses blockchain technology as the underlying technology and represents the application of the blockchain 1.0 era. In the second research phase (2018–2019), the surged keywords consisted of privacy-preserving (the burst strength of privacy-preserving = 4.50), architecture (the burst strength of architecture = 8.33) and electronic health record (the burst strength of electronic health record = 4.49). This demonstrates that the second research phase broadens the research themes of the first phase, and leverages the value of blockchain technology in concrete applications. In the last research phase (2020–2021), the mainstream research topics

included "entrepreneurship" (the burst strength of entrepreneurship = 2.87, 2020–2021), "contract" (the burst strength of contract = 5.82, 2020–2021), "industrial internet" (the burst strength of industrial internet = 3.47, 2020–2021), "data management" (the burst strength of data management = 2.87, 2020–2021) and "distributed ledger technology" (the burst strength of distributed ledger technology = 2.87, 2020–2021), all of which represent the further expansion of blockchain application scenarios.

3.3. Qualitative Analysis

3.3.1. Other Research Topics of Blockchain Research

The fact that the six research hotspots were ascertained through quantitative analysis merits attention. However, important subjects may be neglected because they did not have a high number of citations [29]. This research adopted a three-step procedure for qualitative analysis to find other important subjects of blockchain research, which is shown in Figure 5.

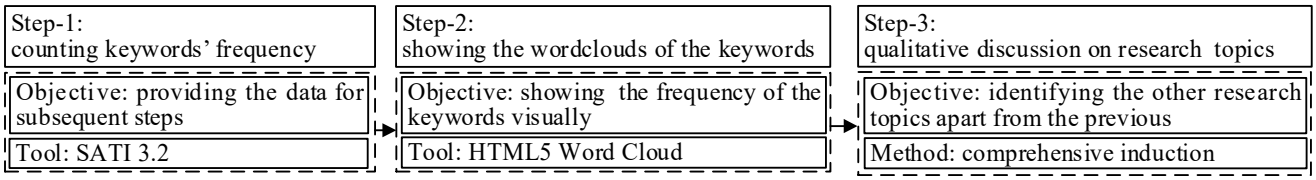

Figure 5. The three-step workflow for the qualitative analysis.

In addition, keywords could be utilized to detect research hot topics within the scientific community, and it have also been used in previous research [29]. Therefore, to find other topics in the blockchain research field, we used the Statistical Analysis Toolkit for Informatics 3.2 (SATI3.2) to count keyword frequencies of all 4329 literature publications in step 1. Based on the above frequencies, we drew the word cloud of the keywords (see Figure 6) in step 2. Finally, combining the keyword size and position in Figure 6, and using professional experience, we recognized the other research subjects in the blockchain research field in step 3; these consisted of the Internet of thing (frequency = 321), access control (frequency = 148) and trust (frequency = 164).

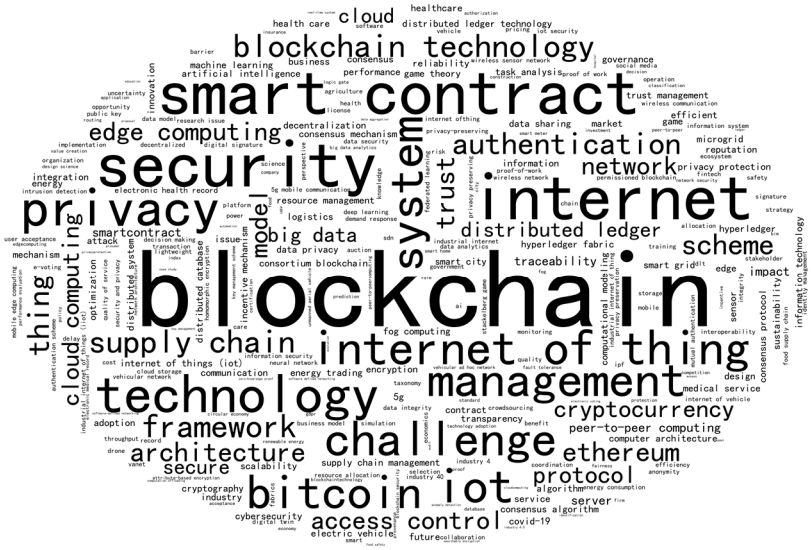

Figure 6. The word cloud of blockchain research keywords.

Enabled by the latest developments in RFID (radio-frequency identification) technology, smart sensors, communication technologies and Internet protocols, the Internet of things is rapidly finding its way into our modern lives, and aims to improve our quality of life by connecting many smart devices, technologies and applications. As pointed

out previously, the Internet of things is expected to bridge diverse technologies (such as blockchain technology). By combining information-sensing devices with the network, new technologies will be generated to support strategic decisions [98].Therefore, it is popular to discuss the critical role of blockchain technology in various application scenarios of the Internet of things [99,100]. In addition, the success of the IoT revolution depends on many key challenges, such as security and privacy [101], so effective access control mechanisms must be defined and implemented to protect privacy. In order to allow users better control of their own data, Ouaddah et al. [102] created a completely decentralized privileged-management framework for anonymity and privacy protection. Within this framework, FairAccess was introduced, and it opened up a new area of applicability for blockchain-access control. As for trust, it is confirmed that trust plays a key and complex role in sharing economic interactions [103], while the trust-free system created by blockchain promises to revolutionize peer-to-peer interactions that require a high level of trust. In such trust-free system, blockchain technology is used to automatically create an immutable, consensually agreed, and publicly available record of past transactions, which is governed by the whole system to mitigate trust issues in transaction systems [104]. As a result, it is popular to discuss the roles of blockchain technology in ensuring trust during transaction processes.

According to the above discussion, three other research topics have been identified through qualitative analysis, which consists of the Internet of things, access control and trust.

3.3.2. Current Research Gaps in Blockchain Research

Based on the relevant content analysis of blockchain study from 2015 to 2021, we identified two research gap which have had a lack of investigation and need more attention. The first one is the true effect of blockchain technology on firms' operational efficiency. As discussed in hotspot 1, blockchain technology is widely applied in various scenarios, due to its decentralization and trust-free feature, driving the transformation of the industrial economy into an information economy. However, most research evaluating the effect of blockchain technology on firms' operational efficiency is based on a single project case [11,105], which is not universal for all fields and projects. Generally speaking, firms' operational efficiency is the combination of results caused by multiple factors, including energy use, technological innovation and policy coordination [106]. Therefore, the true effect of blockchain technology on firms' operational efficiency needs to be investigated independently, under the condition that other conditions are controlled and unchanged. The second research gap is the regulation on the "dark sides" of blockchain technology. As discussed in hotspot 1 and 2, plenty of technical applications based on blockchain technology are promoting social development. However, the illegal applications of blockchain technology are rarely mentioned. As cryptocurrencies are one of the largest unregulated markets in the world, one-quarter of bitcoin users and one-half of bitcoin transactions are associated with illicit activity [107]. Allman [108] has revealed the process of bitcoin transactions as being associated with illegal activity: bitcoin's anonymous trading methods, with cryptocurrencies drawing value from illegal markets, money laundering, the "darknet" (the online black market), and initial coin offerings, present challenges for regulators. In addition, it is pointed out that terrorists and criminals have exploited bitcoin's P2P and pseudo-anonymous nature in furtherance of their illicit activities [109,110]. These problems are related to the lack of legal and personnel supervision of blockchain, which is decentralized, and the fact that the transaction records are difficult to change [111]. Consequently, in order to further crack down on fraud and other illegal acts against consumers and market interests, the United States, China, Britain, Japan, and Switzerland have proposed corresponding regulatory methods to manage blockchain technology [112]. However, it is pointed out that bitcoin is still absolutely unrestricted in approximately 110 countries and that since bitcoin is new, the government and banks have not applied any corresponding

policies to it [111]. Therefore, more research focusing on the regulation of the technology will be published, to overcome these dark sides of blockchain technology.

4. Tentative Conclusions

4.1. Overview

The present research combines quantitative analysis (i.e., scientometric analysis) with qualitative analysis (i.e., content analysis) to identify the research hotspots, research frontiers and evolutionary paths of blockchain research from 2015 to 2021, and to identify the research gaps for future research. To achieve these goals, we designed and adopted a four-sub-step research procedure, consisting of data collection, descriptive analysis, quantitative analysis (i.e., scientometric analysis), and qualitative analysis (i.e., content analysis). Based on the data gathered from the WoS core-collection database, we finished the research process, and the conclusions mainly include the following points.

4.1.1. The Current State of Blockchain Research

In terms of source journals, IEEE Access and IEEE Internet of Things Journal were the most impactful journals in the blockchain research field.

As for the academic performances of different stakeholders, countries such as China, the United States, India and England have made tremendous academic contributions to the blockchain research field. The academic institutions, Beijing University of Posts and Telecommunications, Chinese Academy of Sciences, and King Saud University had the most prominent influence. In term of authors, Yan Zhang, Kim-Kwang Raymond Choo and Neeraj Kumar had outstanding influence in this field.

Through document co-citation analysis, Christidis and Devetsikiotis [42], Zheng et al. (2017) [25] and Zheng et al. (2018) [42] were found to be in the top three of all documents in terms of importance degree. Through quantitative and qualitative analyses, nine research questions were identified: the specific application areas of blockchain technology, the integration of blockchain and other technologies, the driving factors of blockchain, the values of blockchain technology, the types of blockchain, the core technologies of blockchain, the Internet of things, access control and trust.

4.1.2. The Research Frontiers and Openness of Blockchain Research

Five research frontiers were identified through keyword-burst analysis, consisting of entrepreneurship, contract, industrial internet, data management and distributed ledger technology. Furthermore, three phases of blockchain research were summarized in a comprehensive summary: the first stage (2015–2017) introduces the product of the blockchain 1.0 era (bitcoin); the second stage (2018–2019) represents the specific application areas of blockchain; and the third stage (2020–2021) extends the scope of the research and application scenarios, which also represent the research frontiers.

Two research gaps in the blockchain field were identified by the qualitative analysis, namely the true effect of blockchain technology on firms' operational efficiency and the regulation of the "dark sides" of blockchain technology. These themes deserve more attention from researchers and practitioners in the blockchain research field.

4.2. Limitations and Recommendations

This research may have some limitations. Firstly, the completeness of the data adopted in the present research may be limited. Although the WoS database used in the resent research is considered to be the core database, because of its most authoritative publications, and has been used as the only database in many bibliometric articles in many fields, the present research might still have neglected some important literature that is outside of the WoS database. In addition, since the data collection of this research was conducted on 1 January 2022, there may not have been enough time for recently published articles to be referenced and to appear in the quantitative and qualitative analysis Therefore, the

conclusions drawn from the data might also be restricted. Subsequent researchers can enrich the data source and take into account the valuable publications published recently.

Additionally, as has already been pointed out, misspellings, incoherence, and homophones can also make bibliometric studies fail [113]. As a result, even though the data used in this study went through two rounds of screening, it is inevitable that this research has used a very small amount of irrelevant data. Thus, future research in this area could refine the data-screening process and improve data quality.

Finally, this research gives an overview of blockchain research by showing 18 effective thematic clusters. However, as a literature review, this research cannot be expected to identify research problems and make research hypotheses about blockchain. Future research could pay attention to the application effect of blockchain in these thematic clusters by using empirical analysis.

Author Contributions: Conceptualization, X.L.; methodology, X.L. and R.Z.; software, L.C.; validation, X.L., H.J. and L.C.; formal analysis, X.L. and L.C.; investigation, H.J.; resources, X.L., W.M. and R.Z.; data curation, W.M. and R.Z.; writing—original draft preparation, X.L. and H.J.; writing—review and editing, X.L. and L.C.; visualization, L.C.; supervision, Y.Y. and H.L.; project administration, W.M. and R.Z.; funding acquisition, H.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Key Science and Technology Projects of Henan Province (NO.222102320174); the National Social Science Foundation of China: (NO.21BGL029); and the National Natural Science Foundation of China (NO.72271091; No.71974056).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data available on request from the authors.

Acknowledgments: We thank anonymous reviewers for comments and suggestions that greatly improved the manuscript.

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

References

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 7 February 2022).
2. Raikwar, M.; Gligoroski, D.; Kralevska, K. SoK of Used Cryptography in Blockchain. *IEEE Access* **2019**, *7*, 148550–148575. [CrossRef]
3. Raman, R.K.; Varshney, L.R. Distributed Storage Meets Secret Sharing on the Blockchain. In Proceedings of the 2018 Information Theory and Applications Workshop (ITA), San Diego, CA, USA, 11–16 February 2018; pp. 1–6. [CrossRef]
4. Xu, G.; Liu, Y.; Khan, P.W. Improvement of the DPoS Consensus Mechanism in Blockchain Based on Vague Sets. *IEEE Trans. Ind. Inform.* **2019**, *16*, 4252–4259. [CrossRef]
5. Frizzo-Barker, J.; Chow-White, P.A.; Adams, P.R.; Mentanko, J.; Ha, D.; Green, S. Blockchain as a disruptive technology for business: A systematic review. *Int. J. Inf. Manag.* **2019**, *51*, 102029. [CrossRef]
6. Cong, L.W.; He, Z. Blockchain Disruption and Smart Contracts. *Rev. Financ. Stud.* **2019**, *32*, 1754–1797. [CrossRef]
7. Skowroński, R. The open blockchain-aided multi-agent symbiotic cyber–physical systems. *Futur. Gener. Comput. Syst.* **2019**, *94*, 430–443. [CrossRef]
8. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.-K.R. A systematic literature review of blockchain cyber security. *Digit. Commun. Netw.* **2020**, *6*, 147–156. [CrossRef]
9. Crosby, M.; Pattanayak, P.; Verma, S.; Kalyanaraman, V. Blockchain technology: Beyond bitcoin. *Appl. Innov.* **2016**, *2*, 71.
10. Rajasekhar, K.; HarshiniYalavarthy, S.; Mullapudi, S.; Gowtham, M. Redactable blockchain and it's implementation in bitcoin. *Int. J. Eng. Technol.* **2018**, *7*, 401–405. [CrossRef]
11. Wang, Z.; Wang, T.; Hu, H.; Gong, J.; Ren, X.; Xiao, Q. Blockchain-based framework for improving supply chain traceability and information sharing in precast construction. *Autom. Constr.* **2019**, *111*, 103063. [CrossRef]
12. Akdoğan, D.A.; Kurular GY, S.; Geyik, O. Cryptocurrencies and blockchain in 4th industrial revolution process: Some public policy recommendations. In *Globalisation & Public Policy*; IJOPEC: London, UK, 2019; pp. 79–92.
13. Kar, A.K.; Navin, L. Diffusion of blockchain in insurance industry: An analysis through the review of academic and trade literature. *Telemat. Inform.* **2020**, *58*, 101532. [CrossRef]

14. Tarr, J.A. Distributed ledger technology, blockchain and insurance: Opportunities, risks and challenges. *Insur. Law J.* **2018**, *29*, 254–268.
15. Zhang, L.; Xie, Y.; Zheng, Y.; Xue, W.; Zheng, X.; Xu, X. The challenges and countermeasures of blockchain in finance and economics. *Syst. Res. Behav. Sci.* **2020**, *37*, 691–698. [CrossRef]
16. Eyal, I. Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities. *Computer* **2017**, *50*, 38–49. [CrossRef]
17. Wang, Y.; Singgih, M.; Wang, J.; Rit, M. Making sense of blockchain technology: How will it transform supply chains? *Int. J. Prod. Econ.* **2019**, *211*, 221–236. [CrossRef]
18. Kamble, S.; Gunasekaran, A.; Arha, H. Understanding the Blockchain technology adoption in supply chains-Indian context. *Int. J. Prod. Res.* **2018**, *57*, 2009–2033. [CrossRef]
19. McGhin, T.; Choo KK, R.; Liu, C.Z.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 62–75. [CrossRef]
20. Nawari, N.O.; Ravindran, S. Blockchain and building information modeling (bim): Review and applications in post-disaster recovery. *Buildings* **2019**, *9*, 149. [CrossRef]
21. Cai, Y.; Zhu, D. Fraud detections for online businesses: A perspective from blockchain technology. *Financ. Innov.* **2016**, *2*, 20. [CrossRef]
22. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L. A Systematic Review of the Use of Blockchain in Healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]
23. Bodkhe, U.; Tanwar, S.; Parekh, K.; Khanpara, P.; Tyagi, S.; Kumar, N.; Alazab, M. Blockchain for industry 4.0: A comprehensive review. *IEEE Access* **2020**, *8*, 79764–79800. [CrossRef]
24. Kim, H.; Kim, J.; Jang, K.; Han, J. Are the Blockchain-Based Patents Sustainable for Increasing Firm Value? *Sustainability* **2020**, *12*, 1739. [CrossRef]
25. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
26. Guo, J.; Cengiz, K.; Tomar, R. An IOT and Blockchain Approach for Food Traceability System in Agriculture. *Scalable Comput. Pract. Exp.* **2021**, *22*, 127–137. [CrossRef]
27. Chen, C.; Hu, Z.; Liu, S.; Tseng, H. Emerging trends in regenerative medicine: A scientometric analysis in CiteSpace. *Expert Opin. Biol. Ther.* **2012**, *12*, 593–608. [CrossRef] [PubMed]
28. Zhao, X.; Zuo, J.; Wu, G.; Huang, C. A bibliometric review of green building research 2000–2016. *Archit. Sci. Rev.* **2019**, *62*, 74–88. [CrossRef]
29. Li, X.; Zhang, R.; Yin, Y.; Deng, J. Reviewing Global Relational Governance Research from 2002 to 2020. *J. Business-to-Business Mark.* **2021**, *28*, 421–439. [CrossRef]
30. Sun, Z.; Wang, Y.; Cai, Z.; Liu, T.; Tong, X.; Jiang, N. A two-stage privacy protection mechanism based on blockchain in mobile crowdsourcing. *Int. J. Intell. Syst.* **2021**, *36*, 2058–2080. [CrossRef]
31. Chen, C.; Dubin, R.; Kim, M.C. Orphan drugs and rare diseases: A scientometric review (2000–2014). *Expert Opin. Orphan Drugs* **2014**, *2*, 709–724. [CrossRef]
32. Li, X.; Wu, P.; Shen, G.Q.; Wang, X.; Teng, Y. Mapping the knowledge domains of Building Information Modeling (BIM): A bibliometric approach. *Autom. Constr.* **2017**, *84*, 195–206. [CrossRef]
33. Popescu, D.V.; Dima, A.; Radu, E.; Dobrota, E.M.; Dumitrache, V.M. Bibliometric Analysis of the Green Deal Policies in the Food Chain. *Amfiteatru Econ.* **2022**, *24*, 62. [CrossRef]
34. Dima, A.; Bugheanu, A.M.; Boghian, R.; Madsen, D.Ø. Mapping Knowledge Area Analysis in E-Learning Systems Based on Cloud Computing. *Electronics* **2022**, *12*, 62. [CrossRef]
35. Song, J.; Li, Y.; Feng, Z.; Wang, H. Cluster Analysis of the Intellectual Structure of PPP Research. *J. Manag. Eng.* **2019**, *35*, 04018053. [CrossRef]
36. Yong, Y.; Feiyue, W. Development status and Prospect of block chain technology. *Acta Autom. Sin.* **2016**, *42*, 481–494.
37. Pankova, N. Blockchain-Based Genomics for Precision Medicine. In *Public Health Genomics*; Karger: Basel, Switzerland, 2018; Volume 21, p. 9.
38. Serra-Navarro, D. On Blockchain and Art: An interview with Ruth Catlow. *Arte Individ. y Soc.* **2019**, *31*, 969–976. [CrossRef]
39. Wu, F.; Geng, Y.; Tian, X.; Zhong, S.; Wu, W.; Yu, S.; Xiao, S. Responding climate change: A bibliometric review on urban environmental governance. *J. Clean. Prod.* **2018**, *204*, 344–354. [CrossRef]
40. Sun, Y.; Zhai, Y. Mapping the knowledge domain and the theme evolution of appropriability research between 1986 and 2016: A scientometric review. *Scientometrics* **2018**, *116*, 203–230. [CrossRef]
41. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
42. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
43. Zyskind, G.; Nathan, O. Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the Security and Privacy Workshops (SPW), San Jose, CA, USA, 21–22 May 2015; pp. 180–184. [CrossRef]

44. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. *arXiv* **2018**, arXiv:1801.10228.
45. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: Theblockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the 37th IEEE Symposium on Security & Privacy 2016, San Jose, CA, USA, 22–26 May 2016.
46. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Using Blockchain for Medical Data Access and Permission Management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30. [CrossRef]
47. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; Shen, L. Blockchain technology and its relationships to sustainable supply chain management. *Int. J. Prod. Res.* **2019**, *57*, 2117–2135. [CrossRef]
48. Aitzhan, N.Z.; Svetinovic, D. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 840–852. [CrossRef]
49. Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where Is Current Research on Blockchain Technology?—A Systematic Review. *PLoS ONE* **2016**, *11*, e0163477. [CrossRef] [PubMed]
50. Chen, C.; Ibekwe-SanJuan, F.; Hou, J. The structure and dynamics of cocitation clusters: A multiple-perspective cocitation analysis. *J. Am. Soc. Inf. Sci. Technol.* **2010**, *61*, 1386–1409. [CrossRef]
51. Khanna, T.; Nand, P.; Bali, V. Permissioned blockchain model for end-to-end trackability in supply chain management. *Int. J. e-Collab. (IJeC)* **2020**, *16*, 45–58. [CrossRef]
52. Sabir, B.E.; Youssfi, M.; Bouattane, O.; Allali, H. Towards a new model to secure IoT-based smart home mobile agents using blockchain technology. *Eng. Technol. Appl. Sci. Res.* **2020**, *10*, 5441–5447. [CrossRef]
53. Miao, Y.; Huang, Q.; Xiao, M.; Li, H. Decentralized and Privacy-Preserving Public Auditing for Cloud Storage Based on Blockchain. *IEEE Access* **2020**, *8*, 139813–139826. [CrossRef]
54. Sharma, P.; Jindal, R.; Borah, M.D. Blockchain technology for cloud storage: A systematic literature review. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–32. [CrossRef]
55. Zhang, P.; Shilin, L.I.; Yiming LI, U.; Xiaoqi QI, N.; Xiaodong, X.U. Resource management in blockchain-enabled heterogeneous edge computing system. *J. Commun.* **2020**, *41*, 1–14.
56. Mitani, T.; Otsuka, A. Traceability in Permissioned Blockchain. *IEEE Access* **2020**, *8*, 21573–21588. [CrossRef]
57. Guo, X.; Guo, Q.; Liu, M.; Wang, Y.; Ma, Y.; Yang, B. A Certificateless Consortium Blockchain for IoTs. In Proceedings of the 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), Singapore, Singapore, 29 November–1 December 2020; pp. 496–506. [CrossRef]
58. Tan, H.; Kim, P.; Chung, I. Practical Homomorphic Authentication in Cloud-Assisted VANETs with Blockchain-Based Healthcare Monitoring for Pandemic Control. *Electronics* **2020**, *9*, 1683. [CrossRef]
59. Kalla, A.; Hewa, T.; Mishra, R.A.; Ylianttila, M.; Liyanage, M. The Role of Blockchain to Fight Against COVID-19. *IEEE Eng. Manag. Rev.* **2020**, *48*, 85–96. [CrossRef]
60. Patil, A.S.; Hamza, R.; Hassan, A.; Jiang, N.; Yan, H.; Li, J. Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts. *Comput. Secur.* **2020**, *97*, 101958. [CrossRef]
61. Mwitende, G.; Ali, I.; Eltayieb, N.; Wang, B.; Li, F. Authenticated key agreement for blockchain-based WBAN. *Telecommun. Syst.* **2020**, *74*, 347–365. [CrossRef]
62. Cui, Z.; Fei XU, E.; Zhang, S.; Cai, X.; Cao, Y.; Zhang, W.; Chen, J. A hybrid blockchain-based identity authentication scheme for multi-WSN. *IEEE Trans. Serv. Comput.* **2020**, *13*, 241–251. [CrossRef]
63. Deng, S.; Cheng, G.; Zhao, H.; Gao, H.; Yin, J. Incentive-Driven Computation Offloading in Blockchain-Enabled E-Commerce. *ACM Trans. Internet Technol.* **2020**, *21*, 1–19. [CrossRef]
64. Harish, A.R.; Liu, X.L.; Zhong, R.Y.; Huang, G.Q. Log-flock: A blockchain-enabled platform for digital asset valuation and risk assessment in E-commerce logistics financing. *Comput. Ind. Eng.* **2021**, *151*, 107001. [CrossRef]
65. Zuo, Y. Making smart manufacturing smarter—A survey on blockchain technology in Industry 4.0. *Enterp. Inf. Syst.* **2021**, *15*, 1323–1353. [CrossRef]
66. Aste, T.; Tasca, P.; Di Matteo, T. Blockchain Technologies: The Foreseeable Impact on Society and Industry. *Computer* **2017**, *50*, 18–28. [CrossRef]
67. Tanwar, S.; Kaneriya, S.; Kumar, N.; Zeadally, S. *ElectroBlocks*: A blockchain-based energy trading scheme for smart grid systems. *Int. J. Commun. Syst.* **2020**, *33*, e4547. [CrossRef]
68. Mengelkamp, E.; Notheisen, B.; Beer, C.; Dauer, D.; Weinhardt, C. A blockchain-based smart grid: Towards sustainable local energy markets. *Comput. Sci.-Res. Dev.* **2018**, *33*, 207–214. [CrossRef]
69. Huh, J.-H.; Kim, S.-K. The Blockchain Consensus Algorithm for Viable Management of New and Renewable Energies. *Sustainability* **2019**, *11*, 3184. [CrossRef]
70. Tsao, Y.-C.; Thanh, V.-V. Toward blockchain-based renewable energy microgrid design considering default risk and demand uncertainty. *Renew. Energy* **2021**, *163*, 870–881. [CrossRef]
71. Gao, F.; Chen, D.-L.; Weng, M.-H.; Yang, R.-Y. Revealing Development Trends in Blockchain-Based 5G Network Technologies through Patent Analysis. *Sustainability* **2021**, *13*, 2548. [CrossRef]
72. Lin, I.C.; Liao, T.C. A survey of blockchain security issues and challenges. *Int. J. Netw. Secur.* **2017**, *19*, 653–659.

73. Ciatto, G.; Mariani, S.; Maffi, A.; Omicini, A. Blockchain-Based Coordination: Assessing the Expressive Power of Smart Contracts †. *Information* **2020**, *11*, 52. [CrossRef]
74. Macrinici, D.; Cartofeanu, C.; Gao, S. Smart contract applications within blockchain technology: A systematic mapping study. *Telemat. Inform.* **2018**, *35*, 2337–2354. [CrossRef]
75. Kufeoglu, S.; Zkuran, M. Energy consumption of bitcoin mining. *Camb. Work. Pap. Econ.* **2019**, *10*, 525–529.
76. Hosseinian, H.; Shahinzadeh, H.; Gharehpetian, G.B.; Azani, Z.; Shaneh, M. Blockchain outlook for deployment of IoT in distribution networks and smart homes. *Int. J. Electr. Comput. Eng. (IJECE)* **2020**, *10*, 2787–2796. [CrossRef]
77. Tikhomirov, S. Ethereum: State of knowledge and research perspectives. In *International Symposium on Foundations and Practice of Security*; Springer: Cham, Switzerland, 2017; pp. 206–221.
78. Marbouh, D.; Abbasi, T.; Maasmi, F.; Omar, I.A.; Debe, M.S.; Salah, K.; Jayaraman, R.; Ellahham, S. Blockchain for COVID-19: Review, opportunities, and a trusted tracking system. *Arab. J. Sci. Eng.* **2020**, *45*, 9895–9911. [CrossRef] [PubMed]
79. Fernandez-Carames, T.M.; Fraga-Lamas, P. A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories. *IEEE Access* **2019**, *7*, 45201–45218. [CrossRef]
80. Vranken, H. Sustainability of bitcoin and blockchains. *Curr. Opin. Environ. Sustain.* **2017**, *28*, 1–9. [CrossRef]
81. Mollah, M.B.; Zhao, J.; Niyato, D.; Lam, K.-Y.; Zhang, X.; Ghias, A.M.Y.M.; Koh, L.H.; Yang, L. Blockchain for Future Smart Grid: A Comprehensive Survey. *IEEE Internet Things J.* **2020**, *8*, 18–43. [CrossRef]
82. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom workshops) 2017, Kona, HI, USA, 13–17 March 2017; pp. 618–623.
83. Yang, A.; Xu, J.; Weng, J.; Zhou, J.; Wong, D.S. Lightweight and Privacy-Preserving Delegatable Proofs of Storage with Data Dynamics in Cloud Storage. *IEEE Trans. Cloud Comput.* **2018**, *9*, 212–225. [CrossRef]
84. Li, J.; Wu, J.; Chen, L. Block-secure: Blockchain based scheme for secure P2P cloud storage. *Inf. Sci.* **2018**, *465*, 219–231. [CrossRef]
85. Zhang, Y.; Xu, C.; Lin, X.; Shen, X.S. Blockchain-based public integrity verification for cloud storage against procrastinating auditors. *IEEE Trans. Cloud Comput.* **2019**, *29*, 923–937. [CrossRef]
86. Gawali, M.; Shinde, S.K. Task scheduling and resource allocation in cloud computing using a heuristic approach. *J. Cloud Comput.* **2018**, *7*, 4. [CrossRef]
87. Chen, W.; Zheng, Z.; Ngai, E.C.-H.; Zheng, P.; Zhou, Y. Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum. *IEEE Access* **2019**, *7*, 37575–37586. [CrossRef]
88. Wang, B.; Li, Z. Healthchain: A Privacy Protection System for Medical Data Based on Blockchain. *Future Internet* **2021**, *13*, 247. [CrossRef]
89. Hammi, M.T.; Hammi, B.; Bellot, P.; Serhrouchni, A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Comput. Secur.* **2018**, *78*, 126–142. [CrossRef]
90. Mishra, R.; Bhanodiya, P. A review on steganography and cryptography. In Proceedings of the 2015 International Conference on Advances in Computer Engineering and Applications, Ghaziabad, India, 19–20 March 2015; pp. 119–122.
91. Werbach, K. Trust, but verify: Why the Blockchain needs the law. *Berkeley Technol. Law J.* **2018**, *33*, 487–550.
92. Ma, Z.; Huang, W.; Bi, W.; Gao, H.; Wang, Z. A master-slave blockchain paradigm and application in digital rights management. *China Commun.* **2018**, *15*, 174–188. [CrossRef]
93. Zeng, X.; Hao, N.; Zheng, J.; Xu, X. A consortium blockchain paradigm on hyperledger-based peer-to-peer lending system. *China Commun.* **2019**, *16*, 38–50. [CrossRef]
94. Szabo, N. Smart contracts: Building blocks for digital markets. *EXTROPY J. Transhumanist Thought* **1996**, *18*, 28.
95. Kemmoe, V.Y.; Stone, W.; Kim, J.; Kim, D.; Son, J. Recent Advances in Smart Contracts: A Technical Overview and State of the Art. *IEEE Access* **2020**, *8*, 117782–117801. [CrossRef]
96. Zhang, T.; Li, J.; Jiang, X. Supply chain finance based on smart contract. *Procedia Comput. Sci.* **2021**, *187*, 12–17. [CrossRef]
97. Upadhyay, A.; Mukhuty, S.; Kumar, V.; Kazancoglu, Y. Blockchain technology and the circular economy: Implications for sustainability and social responsibility. *J. Clean. Prod.* **2021**, *293*, 126130. [CrossRef]
98. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutorials* **2015**, *17*, 2347–2376. [CrossRef]
99. Rejeb, A.; Keogh, J.G.; Treiblmaier, H. Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management. *Futur. Internet* **2019**, *11*, 161. [CrossRef]
100. Cao, B.; Li, Y.; Zhang, L.; Zhang, L.; Mumtaz, S.; Zhou, Z.; Peng, M. When Internet of Things Meets Blockchain: Challenges in Distributed Consensus. *IEEE Netw.* **2019**, *33*, 133–139. [CrossRef]
101. Ekanayake, B.N.; Halgamuge, M.N.; Syed, A. Security and Privacy Issues of Fog Computing for the Internet of Things (IoT). In *Cognitive Computing for Big Data Systems over IoT*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 139–174.
102. Ouaddah, A.; Elkalam, A.A.; Ouahman, A.A. FairAccess: A new Blockchain-based access control framework for the Internet of Things. *Secur. Commun. Networks* **2016**, *9*, 5943–5964. [CrossRef]
103. Mazzella, F.; Sundararajan, A.; D'Espous, V.B.; Möhlmann, M. How Digital Trust Powers the Sharing Economy: The Digitization of Trust. *IESE Insight* **2016**, *26*, 24–31. [CrossRef]
104. Hawlitschek, F.; Notheisen, B.; Teubner, T. The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electron. Commer. Res. Appl.* **2018**, *29*, 50–63. [CrossRef]

105. Li, X.; Wu, L.; Zhao, R.; Lu, W.; Xue, F. Two-layer Adaptive Blockchain-based Supervision model for off-site modular housing production. *Comput. Ind.* **2021**, *128*, 103437. [CrossRef]
106. Koh, L.; Dolgui, A.; Sarkis, J. Blockchain in transport and logistics—Paradigms and transitions. *Int. J. Prod. Res.* **2020**, *58*, 2054–2062. [CrossRef]
107. Foley, S.; Karlsen, J.R.; Putniņš, T.J. Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *Rev. Financ. Stud.* **2019**, *32*, 1798–1853. [CrossRef]
108. Allman, K. The dark side of Bitcoin. *LSJ Law Soc. NSW J.* **2018**, *42*, 28–29.
109. Fletcher, E.; Larkin, C.; Corbet, S. Countering money laundering and terrorist financing: A case for bitcoin regulation. *Res. Int. Bus. Finance* **2021**, *56*, 101387. [CrossRef]
110. Reddy, E.; Minnaar, A. Cryptocurrency: A tool and target for cybercrime. *Acta Criminol. Afr. J. Criminol. Vict.* **2018**, *31*, 71–92.
111. 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. Change* **2020**, *158*, 120166. [CrossRef]
112. Till, B.M.; Peters, A.W.; Afshar, S.; Meara, J.G. From blockchain technology to global health equity: Can cryptocurrencies finance universal health coverage? *BMJ Glob. Health* **2017**, *2*, e000570. [CrossRef]
113. Rossetto, D.E.; Bernardes, R.C.; Borini, F.M.; Gattaz, C.C. Structure and evolution of innovation research in the last 60 years: Review and future trends in the field of business through the citations and co-citations analysis. *Scientometrics* **2018**, *115*, 1329–1363. [CrossRef]