Scientometrics
https://doi.org/10.1007/s11192-019-03170-4

The rise of "blockchain": bibliometric analysis of blockchain study

Ahmad Firdaus[1] · Mohd Faizal Ab Razak[1] · Ali Feizollah[2] · Ibrahim Abaker Targio Hashem[3] · Mohamad Hazim[2] · Nor Badrul Anuar[2]

Received: 3 March 2019

Abstract
The blockchain is a technology which accumulates and compiles data into a chain of multiple blocks. Many blockchain researchers are adopting it in multiple areas. However, there are still lacks bibliometric reports exhibiting the exploration of an in-depth research pattern in blockchain. This paper aims to address that gap by analyzing the widespread of blockchain research activities conducted thus far. This study analyzed the Scopus database by using bibliometric analysis in a pool of more than 1000 articles that were published between 2013 and 2018. In particular, this paper discusses various aspects of blockchain research conducted by researchers globally. This study also focuses on the utilization of blockchain and its consensus algorithms. This bibliometric analysis discovered the following: (1) Blockchain able to solve security issues in internet of things (IoT) and would be an increasing trend in the future; (2) Researchers begin to adopt blockchain in healthcare area; (3) The most active country in blockchain publication is United States, followed by China and Germany; (4) Switzerland and Singapore are two small size countries that published few publications, however receives many citations. (5) Research collaborations between countries increased the research publications except for Canada, India, and Brazil. (6) Keyword analysis revealed that researchers are adopting blockchain to solve problems in multiple categories of the data research area (data privacy, digital storage, the security of data, big data, and distributed database). This study also highlighted the utilization and consensus of the algorithm in blockchain research.

Keywords Blockchain · Bibliometric · Consensus algorithm · Security · Review

Introduction

Computer security is an important element in today's environment. It is used to impede and overcome an imminent threat which has the potential to cause serious damages to the computer system or mobile devices. Security practitioners, for instance, conduct various investigations to optimizing the best features (Feizollah et al. 2015; Mustaffa et al. 2015;

✉ Mohd Faizal Ab Razak
faizalrazak@ump.edu.my

Extended author information available on the last page of the article

Published online: 05 July 2019

Mustaffa and Yusof 2012; Rahouma 2017; Hazim et al. 2018) for predictions in machine learning. Furthermore, they also conduct malware analysis as a measure to combat malware threats by using either static or dynamic analysis (Hazim et al. 2018; Firdaus et al. 2017a, b; Adewole et al. 2017; Razak et al. 2017, 2019; Firdaus and Anuar 2015; Ahmed and Zolkipli 2016). Other than malware, money in digital form or 'Bitcoin' also require higher demand for security, which demands a unique framework.

The 'Bitcoin' is a digital form of money (cryptocurrency) (Bartoletti et al. 2019; Wu et al. 2019; Hellani et al. 2018). It has similar functions as fiat money and is used as a medium to purchase materials, foods, and services (Hughes et al. 2019; Lamiri et al. 2019; Maesa et al. 2019). It adopts a technology called blockchain which offers transparency and decentralization (Essaid et al. 2018; Juhász et al. 2018; Parino et al. 2018; da Silva Filho et al. 2018; Dennis and Disso 2019). This technology excludes third-party involvement (reduce transaction costs), has faster transaction time and a distributed ledger. Various studies have utilized the blockchain technology in various fields of investigation such as security (Yuan et al. 2018), vehicles (Liu et al. 2018) and healthcare (Griggs et al. 2018), (Firdaus et al. 2018). These studies have exhibited the critical need to conduct exploration activities in this domain. Nevertheless, these studies gave lack of attention to the study of bibliometrics. A significant number of articles have focussed on this research area but they mainly report on blockchain research impacts and trends only.

Data science and the library domain utilize bibliometrics as a method to identify the author's activities, publication trends, and country relations. It is also used to acquire the information of progress, growth as well as the insight of specific knowledge. This method contributes to a better association of organization data assets, which are fundamental for its successful and effective utilization of data management (Dehdarirad et al. 2015; Wu et al. 2015; Tahaei et al. 2018). There are numerous advantages of using bibliometrics: (1) Authors are able to validate the centrality of their publication, exploration, and research; (2) Institutions are able to assess the publication and measure the quality and impact; (3) Scientists are able to foresee future research undertakings and the critical effect of research on specific domains; and (4) Analysts are able to assess the developing body of knowledge.

In demonstrating the evolution of the blockchain domain, this paper offers a comprehensive assessment of the blockchain research practices which have been published in the Scopus database, from 2013 to 2018. The methodology involves an appraisal of the blockchain studies, topics, publication patterns, and utilization. To fulfill the aim of this paper, the following research questions are articulated: (1) What is the trend of publication in blockchain study throughout the world? and (2) What information is uncovered from this trend and what are the future directions of blockchain study?

The scope of this bibliometric analysis of blockchain studies are as follows:

(a) The bibliometric assessment of blockchain involves 1119 studies which were extracted from the Scopus database which comprises all types of papers including ISI-indexed.
(b) The experiment assesses blockchain research efforts that are recorded in various types of documents.
(c) This study adopts the dominance factor (DF) rankings to reveal author dominance in publication; it uses the keywords used by the authors in blockchain research and it also concentrates on the citations of the authors involved.
(d) This study further investigates blockchain research among countries throughout the world by evaluating the total number of articles, publications, and citations made within each country.

(e) This study emphasizes two useful network connections: (1) Country collaboration network; (2) Keyword co-occurrences network; and (3) Affiliation collaboration network. These networks are to explore the connection between the countries, keywords, and affiliations.
(f) Finally, this study addresses the inclination of blockchain research by summarizing the blockchain research efforts conducted thus far and then using these to forecast possible future realizations.

The remainder of this paper is organized as follows: Sect. 2 surveys the related bibliometric studies. Section 3 provides the methodology used. Section 4 displays the findings of this paper. Section 5 provides the utilization of blockchain insights by addressing the advantages. Section 6 highlights the consensus algorithms involved in blockchain technology and Sect. 7 concludes the paper.

Related works

Bibliometrics is a current technique which is used to estimate, analyze and visualize the construction of scientific fields (Koskinen et al. 2008). It is engaged for the purpose of describing the expansion of the desired field in a particular area of knowledge (Liu et al. 2018). It entails making an evaluation of publications such as the impact factor, citations, publishers, and countries of publication (Lee 2019; Docampo and Cram 2019; Iefremova et al. 2018). Various studies have applied this method. Table 1 tabulates the list of studies which adopted the bibliometric analysis as an approach which is similar to our paper. Nevertheless, there are some differences between previous studies and our paper.

Table 2 illustrates the differences that exist between this paper and previous studies.

As shown in the table, (Miau and Yang 2018) engaged Lotka's law to measure author productivity. In contrast, the current paper applies to another method called the dominance factor (DF). In addition, this paper also uses two types of network connections—country collaboration, keyword co-occurrences, and affiliation collaboration, which have been omitted by previous studies, as a measure to enhance our bibliometric analysis. To fortify the value of this paper, we further include a review of the consensus algorithm (Mingxiao et al. 2017), presenting multiple types of algorithms such as proof of work (PoW), proof of stake (PoS), byzantine fault tolerance (BFT), proof of elapsed time (PoET), proof of bandwidth (PoB), and proof of authentication (PoAh). To augment the findings of this paper,

Table 1 List of studies that adopted a bibliometric method

References	Fields	Year
Loomes and Van Zanten (2013)	Digestive disease	2013
(Wu et al. 2015)	Land-slide studies	2014
(Dehdarirad et al. 2015)	Women in science and higher education	2015
(Mao et al. 2015)	Biomass energy	2015
(Fahimnia et al. 2015)	Green supply chain	2015
(Razak et al. 2016)	Malware	2016
(Miau and Yang 2018)	Blockchain	2016
This paper	Blockchain	2018

Table 2 Comparison with previous studies

Differences		This paper	Bibliometrics of blockchain (Miau and Yang 2018)	Review of the consensus algorithm (Mingxiao et al. 2017)
Year			2016	2017
Author productivity	Lotka's law		•	
	Dominance factor	•		
Subject		•	•	
Documents		•	•	
Citation		•	•	
Countries		•	•	
Network	Country collaboration	•		
	Keyword co-occurrences	•		
	Affiliation collaboration	•		
Consensus algorithm	PoW	•		•
	PoS	•		•
	DPoS	•		•
	LPoS	•		
	PBFT	•		•
	DBFT	•		
	PoA	•		
	PoET	•		
	PoB	•		

we further include additional types of algorithms such as delegated proof of stake (DPoS), leased proof of stake (LPoS), practical byzantine fault tolerance (pBFT), delegated byzantine fault tolerance (DBFT), and proof of authority (PoA). The section below describes how the bibliometric method was applied.

Methodology

The methodology of this study comprises four phases:(1) Search, (2) Result, (3) Findings, and (4) Analysis. Figure 1 visualizes the methodology and its stages.

The process of this study begins by using "blockchain" as the main keyword in the Scopus database. This is to discover the blockchain research direction and the interest of that database. This study preferred the Scopus database because it contains both the ISI and Scopus indexed rank papers (Oakleaf 2009). Following this, the result phase was able to retrieve a total number of 1119 articles that were published between 2013 and 2018. We concentrated our analysis from 2013 onwards because the blockchain was introduced during that year. In the subsequent phase of our study, we focused on uncovering the information. We focused on various aspects which include looking at various document

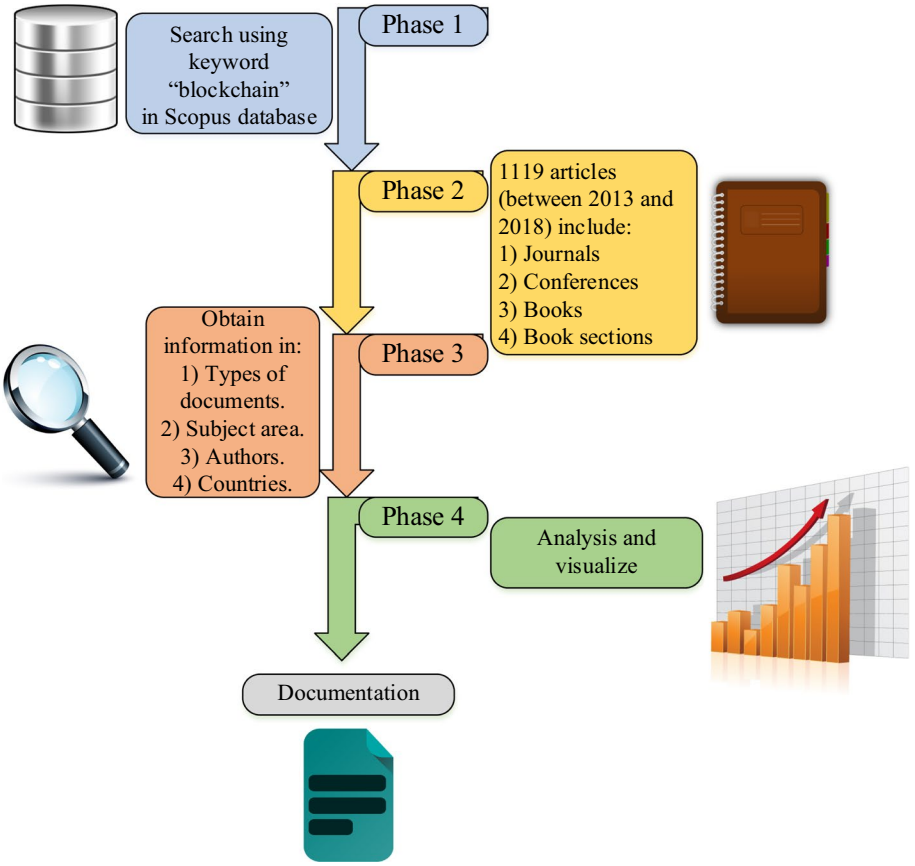

Fig. 1 Methodology stages

types, subject area, authors, and countries. The last phase of our study performed the bibliometric analysis and retrieved the results.

This paper adopted the open source statistical application called R to construct the blockchain bibliometric analysis. Specifically, we installed and used a package known as bibliometrix (Aria and Cuccurullo 2017) which is available in R desktop application. Multiple studies have used this bibliometrix tool for their specific research fields (Cirillo et al. 2018; Brito et al. 2018; Arfaoui et al. 2019). In author's knowledge, this paper is the first study that adopt this tool to run bibliometric analysis in blockchain. The tool is able to provides many blockchain findings and based on it, we made visualizations and analyzed further in the section below.

Bibliometric analysis

The bibliometric analysis of our study is divided into four categories which also carry multiple sub-categories. The main categories are; (1) Types of documents, (2) Subject area, (3) Authors and (4) Countries. The sub-categories developed under Authors were: (a)

Author's dominance, (b) Author's keywords, (c) Total citations, (d) Country's total number of articles, (e) Country's publications, (f) Country's total citations, and (g) Collaboration networks. These findings are important because they generate the bibliometric information which can be used to unravel high impact research that contributes to generating new knowledge for blockchain. Table 3 tabulates the information extracted from the Scopus database, with 1119 articles published between 2013 and 2018 (May 2018).

As can be seen, these articles were written in 475 sources consisting of journals, books, conferences, and proceedings. The keywords noted in the articles were twice the number of the articles, totaling 2024. The number of authors identified from the articles totaled 2227, with 145 single authors in each article and the rest (2082) were articles with multiple authors in each article. From the year 2013 to May 2018, results showed the number of articles increasing rapidly. It is expected that by the end of 2018, this number would increase even more steadily. To display visually, Fig. 2 depicts Table 3 information in a graph form. The next section elaborates on the sources of the articles and their numbers.

Type of documents

Figure 3 provides information to analyze the different types of documents. It elaborates on the outcomes according to placements. Here, it can be seen that conference papers carried a total of 564 documents, noted to be the highest ranking among the others, followed by Journal Articles which carried a total of 315 documents and Conference Reviews, carrying a total of 101 documents.

Table 3 Main information

Main information	Explanation	No.
Articles	Total number of articles	1119
Sources (Journals, Books, etc.)	The frequency distribution of sources (journals, books, etc.)	475
Author's Keywords	Total number of keywords	2024
Authors		
Authors	The authors' frequency distribution	2227
Author Appearances	The number of author appearances	3220
Authors of single authored articles	The number of single author per articles	145
Authors of multi authored articles	The number of authors of multi authored articles	2082
Other		
Authors per Article	Average number of authors in each article	1.99
Co-Authors per Articles	Average number of co-authors in each article	2.88
Average citations per article	Average number of citation in each article	1.859
Collaboration Index		2.56
Year		
2013	Number of articles in each year	2
2014		8
2015		37
2016		165
2017		663
2018		244

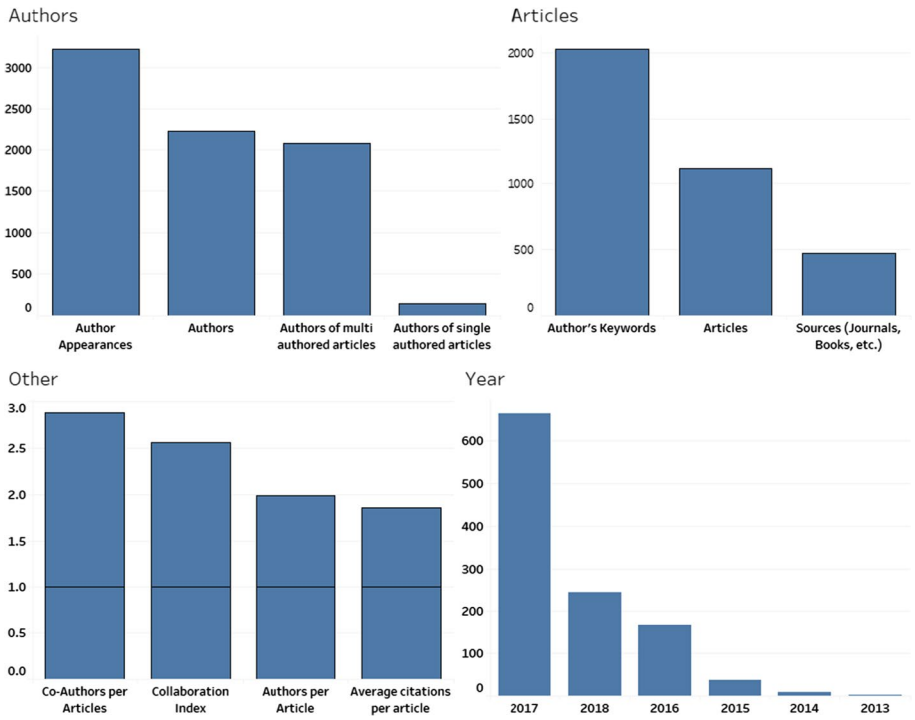

Fig. 2 Main information in figure form

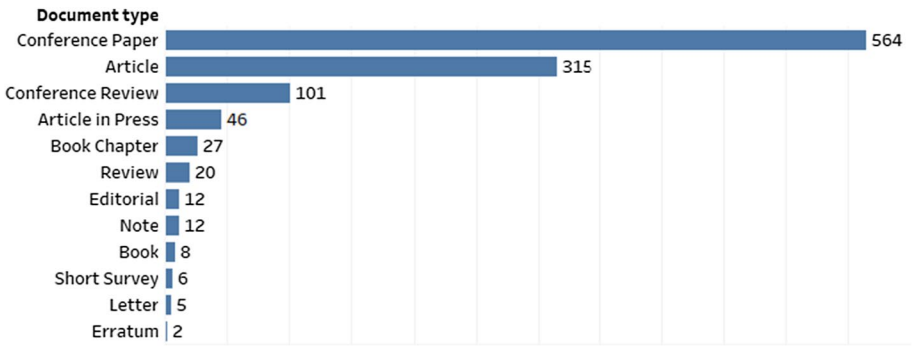

Fig. 3 Type of documents

Figure 3 envisages a trend that blockchain researchers were most interested in publishing conference papers which are in the form of proceedings, rather than an accumulation of papers that were published in websites or in book form. The reason is, these conference papers were submitted before the conference event, and in this manner, the papers become available to all the participants. This situation allows the readers to understand the idea behind the papers and where possible, to submit their feedback after the presentation of the papers when the conference ends. Based on this, the authors of the conference papers are then able to improve and revise their research ideas based

on significant feedback. Therefore, conference publications before the conference are much more useful as it allows the readers to read multiple times and to understand the research in detail. Following this, the blockchain authors are able to retrieve the audience feedbacks much better during the conference event. Table 4 and Fig. 4 show that lecture note is the first place chosen by blockchain researchers to publish their conference papers.

Lecture notes appear to be the platform where many of the authors submitted their conferences papers. The table tabulates that it received many publications in conferences when compared to journal articles. As such, (Garcia-Alfaro et al. 2017) refers to the Lecture Notes in Computer Science that is contained in the proceedings of the First International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2017) held in Oslo, Norway, on September 14, 2017, in conjunction with the 22nd European Symposium on Research in Computer Security (ESORICS) 2017. This lecture notes contained many ideas and novel contributions that involved blockchain technologies.

Other than lecture notes, we able to see the occurrences of all the sources (lecture notes, ACM and Ceur workshop) maintain except IEEE Access. The figure above depicts that IEEE Access would mark an increasing value of occurrences in blockchain publication in the future. On the other hand, the subsequent section highlights the subject area that attracted the researchers to adopt the blockchain technology.

Table 4 Sources that involves in the blockchain

Top 20 sources	No.
Lecture notes in computer science including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics	152
ACM international conference proceeding series	36
Ceur workshop proceedings	34
IEEE access	27
Proceedings Of The ACM conference on computer and communications security	16
Advances in intelligent systems and computing	15
Future generation computer systems	11
Strategic change	10
Zhongguo Dianji Gongcheng Xuebao proceedings of the Chinese society of electrical engineering	10
Computer	9
Zidonghua Xuebao Acta Automatica Sinica	9
Economist United Kingdom	8
IT Professional	8
Lecture Notes of the Institute for computer sciences social informatics and telecommunications engineering Inicst	8
Metaphilosophy	8
Business and information systems engineering	7
F1000 research	7
Lecture notes in business information processing	7
Leibniz international proceedings in informatics lipics	7
New economic windows	7

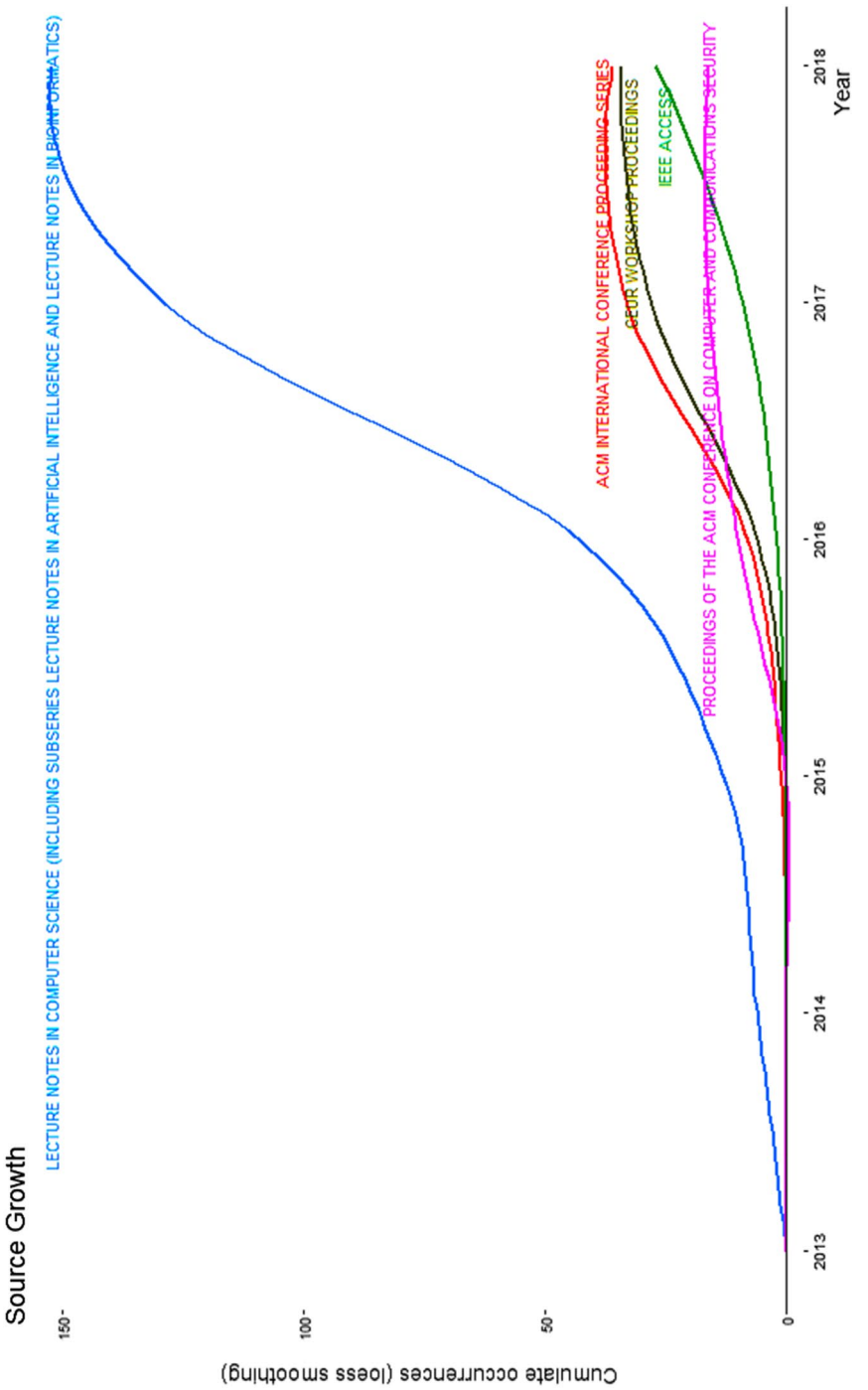

Fig. 4 Source growth

Subject area

Figure 5 depicts the subject area that involved blockchain research. As expected, the subject area that received more attention from researchers was Computer Science, which marked 828 involvements in blockchain technology. Additionally, the combination of the two basic Computer Science subjects, Distributed Computing and Cryptography had also triggered the blockchain innovation.

Distributed computing in computer science area is one of the advantages of the blockchain. Before blockchain existed, the torrent site had utilized this decentralization element which seemed to be functioning admirably well. The setback of the torrent site, however, was that participants were practicing unethical acts. They were posting useless information and uploading malicious applications, without being detected or punished. Moreover, participants in the torrent site who also acted as peers in the network received no incentives when volunteering their own computer in the torrent network. To overcome this disadvantage, the creator of Bitcoin (Satoshi Nakamoto) then developed his own application which was able to limit the power of the participants in the network, but at the same time providing them with incentives by validating the Bitcoin transaction. This led Cryptography to be one of the elements in the blockchain approach.

Cryptography is a practice which secures people's private messages—only the sender and receiver are able to read the messages. To further strengthen the security, two validations are required: (1) Encryption and (2) Decryption. These two methods involve different techniques and encryption keys. A third party is unable to read the private messages transmitted between the sender and receiver without the proper key to decode the encryption. Modern cryptography was developed to incorporate numerous sub-fields in computer science, for instance, data integrity, user authentication, e-commerce, and banking (Kshetri 2017).

The subsequent subject areas of interest are engineering, mathematics, and business and finally, management and accounting. As Bitcoin and blockchain are closely related to economy and mathematics, it was inevitable that business, engineering, and mathematics

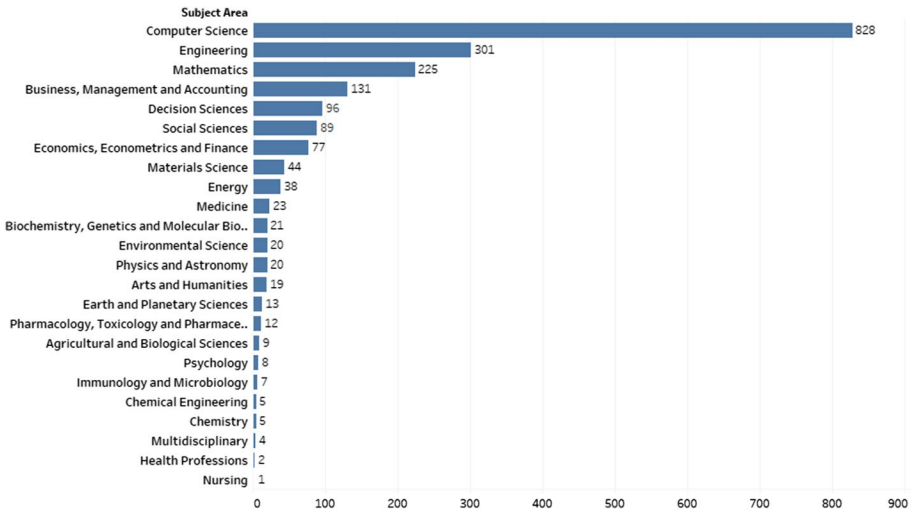

Fig. 5 Subject areas that involve blockchain

would also become the subject areas most involved. This is because engineering and mathematics are subjects that are also included in computer science while business, management, and accounting are excluded. The normal economy would require monetary policies, taxation, voting, fiscal policies, and common security defense. Similarly, Bitcoin also involves inflation (monetary policy), fees (taxation), upgrades (voting), block size (fiscal policy) and network security (common security defense). Bitcoin provides transparency and freedom by employing the decentralization method and this coincides with the centralization that normal banks apply currently.

It is worth to mention that medical and healthcare subject areas are presently combined with blockchain and are receiving keen attention from researchers. The researchers give their trust and believe in the potential of blockchain in involving human lives. Six subject areas related to this include medicine, biochemistry, genetics, and molecular biology, pharmacology, toxicology and pharmaceutical, psychology, immunology and microbiology, health professions and nursing (Griggs et al. 2018; Kuo et al. 2017).

In viewing the healthcare area, one of the problems arise in healthcare is the regulation of the medical data. Currently, the clinical data of patients are digitized but the regulations and rules protecting the data from being shared with others have not been emphasized. Before the invention of the blockchain, the staff of healthcare provider keyed-in the clinical data manually and if regulations allow this such data to be shared, the system may offer inadequate information and there may be errors derived from various manual key-in information. This may derive serious outcomes. However, with the blockchain technology, it able to overcomes this disadvantage. The trusted and unalterable data noted in the distributed ledger provided by blockchain enables the accumulation of information encompassing payers, healthcare providers, and pharmaceutical manufacturers to be gathered together within a safe and trusted environment. The blockchain approach offers hospitals these advantages, thereby saving mankind in the near future. Meanwhile, the subsequent section discusses the author's information who contribute knowledge in blockchain research.

Authors

This section identifies the authors who were most active in blockchain research. To accomplish this, thi section employed the author's keywords, dominance ranking factor, and total citations. Table 5 lists the authors with their published articles in the top 20 rankings.

As seen in the table, Xiwei Xu (Governatori et al. 2018; Han et al. 2018; Lo et al. 2018; Liu et al. 2017, 2018; Xu et al. 2016; Weber et al. 2016; Wang et al. 2018) leads in publication followed by Ingo M. Weber (Rimba et al. 2017, 2018; Mendling et al. 2018a, b, Vladimiro Sassone (De Angelis et al. 2018; Aniello et al. 2017; Margheri 2018), and Shi Elaine (Pass and Shi 2018). These are the top four authors with eleven, nine and eight articles respectively. The remainder of the authors were observed to be publishing eight, seven or six articles in total. Table 5 shows that these authors were involved in publications, either as the main or corresponding author. It is noted that some authors were published as the main author only while others were publishing as co-authors. Therefore, there is a need to measure the contribution power of each author. This is done by investigating the dominance ranking factor through a number of factors in the following section.

Table 5 Authors with a number of articles

Number of articles	Authors (top 20)
11	Xu, Xiwei
9	Weber, Ingo M.
8	Sassone, Vladimiro
	Shi, Elaine
7	Gao, Zhimin
	Kiayias, Aggelos
	Kshetri, Nir
	Margheri, Andrea
	Pass, Rafael
	Shetty, Sachin S.
	Shi, Weidong
	Wattenhofer, Roger P
6	Chen, Lin
	Decker, Christian
	Fujimura, Shigeru
	Liang, Xueping
	Lu, Yang
	Pinna, Andrea
	Staples, Mark D
	Tsai, Wei Tek

Authors' dominance ranking

The dominance factor (DF) is a ratio which measures the fraction of multi-authored articles in which an author acts as the first author (Kumar and Kumar 2008). There were many bibliometric studies which utilized the DF factor in their studies (Wu et al. 2015; Elango and Rajendran 2012). The DF ranking calculates the author's dominance in producing articles. The DF factor is the proportion of a number of multi-authored papers where the author as first author (Nmf) is divided by the total number of multi-authored papers of the author (Nmt). In the single author case, this is omitted due to its constant value of "one" for single authored papers. The mathematical equation for the DF factor is shown as:

$$\mathrm{DF} = \frac{\mathrm{Nmf}}{\mathrm{Nmt}}$$

Table 6 tabulates the list of authors in the top 20 DF ranking and this is led by Pass and Shi (2017). who appeared as a first author in six articles and as one of the many authors in seven multi-authored articles. This ranking continues with Decker C. and Chen L. The result implies that Pass, Decker, and Chen dominate in their research team because they appeared as the first author in all their papers (seven for Pass, six for Decker and seven for Chen, respectively). The tables also indicate that Xu X was ranked 15. Although Xu X appeared to be the top among the eleven multi-authored articles, the DF calculates that Xu X appeared as the first author only in two articles. Figure 6 depicts the outcome into a figure form.

Table 6 Author's dominance

Rank by DF	Author	Dominance factor	Multi authored	First authored	Rank by articles
1	Pass Rafael	0.8571429	7	6	15
2	Decker Christian	0.6666667	6	4	19
3	Chen Lin	0.5714286	7	4	8
4	Liang Xueping	0.5	8	4	5
5	Kiayias Aggelos	0.4285714	7	3	10
6	Wang Jian	0.4285714	7	3	17
7	Kshetri Nir	0.2857143	7	2	11
8	Li Xiaoxin	0.2857143	7	2	12
9	Li Yannan	0.2857143	7	2	13
10	Xu Lei	0.2857143	7	2	18
11	Wang H	0.25	8	2	6
12	Zhang Y	0.25	8	2	7
13	Weber Ingo M.	0.2222222	9	2	3
14	Zhang J	0.2222222	9	2	4
15	Xu Xiwei	0.1818182	11	2	1
16	Fujimura Shigeru	0.1666667	6	1	20
17	Liu J	0.1666667	6	1	21
18	Gao Zhimin	0.1428571	7	1	9
19	Margheri Andrea	0.1428571	7	1	14
20	Shetty Sachin S.	0.1428571	7	1	16

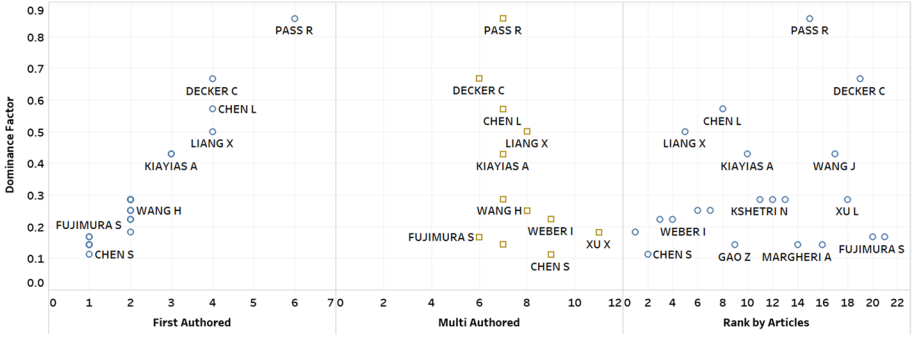

Fig. 6 Dominance factor in figure form

Figure 6 illustrates the dominance factor (DF) followed by the value of first authored, multi authored and rank by articles. As the figure above illustrates, Pass Rafael and Decker Christian are the top domination in DF ranking. A deeper search indicates that Pass Rafael is an Associate Professor in the Massachusetts Institute of Technology (MIT) that has research interests in cryptography and security (Pass 2019). This provides a clear significant proof because cryptography is a backbone of bitcoin digital currency which adopt blockchain mechanism. While Decker Christian is a researcher from ETH Zurich who supervises many students and published multiple publications in bitcoin area (Christian

2019). This evidence shows that their similar interest in bitcoin able to contribute to publishing papers and boost the bitcoin advantages at the same time.

The subsequent section discusses the keywords that authors used in their research articles inclusive of the specific method used and the features or areas displayed in the keywords that are related to the blockchain.

Author's keywords

This section provides the information between keywords and blockchain. The researchers inserted multiple keywords and related it with blockchain in their research articles. This is an important part as we need to analyze the research trends, identify the research gaps in the blockchain area and identify the field of research whereas they have their interest to combined with blockchain.

Table 7 above tabulates the total number of the author's keywords in the top 20 rankings. The ranking is led by blockchain, followed by Bitcoin, privacy and smart contract. The smart contract is similar in purpose to a normal contract in the physical world. It differs in the sense that it is a digital form and is stored within the blockchain system. In particular, a smart contract is a contract that is coded in a software form which stores rules for arranging the terms of an understanding, consequently, confirming satisfaction followed by the execution of the concurred terms. The fundamental thought of the smart contract is to remove the third party while setting up business relations. This means that the involved parties construct the agreement and deal directly with each other.

Table 7 Author's keywords in the blockchain

Author Keywords (top 20)	Articles
Blockchain	572
Bitcoin	168
Privacy	60
Smart contract	58
Cryptocurrency	54
Security	53
Smart contracts	50
Internet of things	47
Ethereum	40
Blockchain technology	32
Iot	32
Access control	21
Trust	17
Decentralization	16
Distributed ledger	16
Cryptography	15
Digital currency	15
Authentication	14
Cloud computing	14
Fintech	13

As an illustration, consider the case of a crowdfunding situation where the project team shares its products and the smart contract gathers money from the supporters. Once the project achieves the objective, the smart contract will distribute the money to the project team according to the agreement of the contract. Alternatively, other than the project development, the smart contract is also capable of another type of agreement such as the sharing of jobs/tasks, gathering of gifts, collecting of donation and setting of goals. In short, people are able to use the smart contract to receive funds until it reaches its goal. However, if the project gets fully funded before the deadline, the money that is raised will automatically go to the product team. If the project fails, the money will automatically go back to the supporters. Besides the smart contract, another area that attracts researchers to combine research with blockchain is the internet of things (IoT).

In Table 7, the keywords that involved multiple small devices (comprising a smartphone, smartwatch, or sensor nodes) is the internet of things (IoT). There are two similar keywords in the IoT, both of which refer to the same subject. One tabulates the "Internet of Things" as 47 and the other tabulates the "IoT" as 32, which is 79 in total. This value of 79 is higher than the keywords of the privacy and smart contract. This outcome proves that the IoT receives more tremendous attention from researchers. Currently, the number of sensor nodes in the IoT keeps on increasing; it is continuously used in vehicles, factory, buildings and modern infrastructure. According to research drawn from the Juniper network, the total amount of IoT sensors and devices is expected to increase to 50 billion by 2022 (Smith 2018). Hence, researchers need to find an initiative to secure the IoT network while at the same time validate the transactional processes (Reyna et al. 2018; Makhdoom et al. 2019). These reasons attract blockchain researchers to conduct experiments and research efforts to combine IoT with blockchain technologies (Reyna et al. 2018; Li et al. 2017).

On the other hand, Fig. 7 visualizes the word TreeMap of keywords that received blockchain interest from researchers. It shows that electronic money, bitcoin, cryptography are the blockchain common keywords. However, other parts of interesting keywords are the internet of things (IoT), information management, health care, and artificial intelligence. This proves that researchers are focused to combine with these fields with blockchain. This indication verifies that the blockchain has potential in securing the IoT sensors, manage well in information management, save lives in the health care field and predict categories or classes with artificial intelligence.

Moreover, in the data point of view, the researchers are depending more faith in the data research area and adopted it with blockchain. The figure above visualizes multiple keywords that relate with data, for instances; (1) data privacy, (2) digital storage, (3) security of data, (4) big data, and (5) distributed the database. This visualization shows that blockchain analyst discover the enormous potential of blockchain in securing important data from privacy and big data.

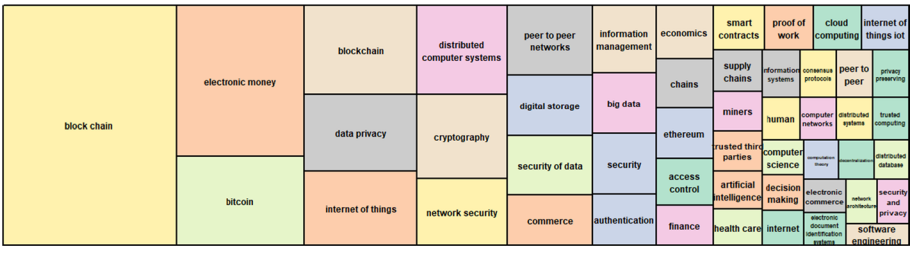

Fig. 7 Word TreeMap

Other than TreeMap, in order to relate these multiple combination keywords in-depth, following figures visualizes a topic dendrogram of keywords with blockchain.

Figure 8 shows a topic dendrogram to observe the hierarchical relationship between keywords that generates from hierarchical clustering. It is used to allocate the objects to clusters by measuring the height of the different objects that joined together in branches. Initially, human in the dendrogram diagram represent the researchers. Other than human, the remainder objects are the keywords in blockchain articles.

The diagram shows that IoT areas are the different branch with cryptocurrency areas (miners, electronic money, bitcoin and proof of work). It highlights that the researchers separate both areas in their research field and shows that they excluding digital money-interest with IoT fields. Instead, they combined IoT with big data, trusted third parties and security. Similar to artificial intelligence (AI), they divide AI from cryptocurrency area and combined it with economic and computer science instead.

Meanwhile, in a security point of view, most of the branches are related to security. The branches that relate with security is IoT, identification systems, peer to peer, and supply chains. This verifies that researchers trust the blockchain and included it in their research to protect IoT data sensors, the identity of people and data of supply information from being attacked. In order to summarize overall keywords, the following figure provides wordcloud to identify the most keywords that attract researches globally.

Figure 9 depicts a wordcloud of keywords included in blockchain article research papers. The general terms in blockchain are highlighted in the figure, such as electronic money, bitcoin, cryptography, and peer to peer networks. However, apart from these general terms, some of the attracted keywords are the internet of things, data privacy, network security, and distributed computer systems. The cloud depicts that blockchain have high potential in these research fields and would mark an increment in amount of blockhain publication in the near future.

Furthermore, the word cloud highlights three areas that involved security, such as; (1) network security, (2) security commerce, and (3) security of data. It highlights that security practitioners have trust in blockchain and adopted it in their respected research field. It also proves that blockchain has the important requirements to protect data from a malicious attempt by the attackers. The cloud also highlights the data area twice; (1) security of data and (2) big data. With the help of blockchain technology, security practitioners adopt blockchain with security research field to protect the data from being breach and access by hackers. Other than word cloud, in the interest to discover which countries have an interest in the keywords, the following section provides the multi-field plot between affiliations and keywords in the top 20 ranking.

Figure 10 depicts that certain universities only adopt blockchain on certain areas only, depends on their expertise. For instances, Zhejiang University is focused on digital currency and cryptocurrency. Meanwhile, the universities that have an interest in smart contract are the University of Edinburgh, University of Cagliari, University of College London, Beihang University and Peking University. While in IoT research, the universities that conducted it with blockchain are most from the Asia (Keio University, University of South Wales, Beijing University, Tsinghua University, and Nanyang Technological University), except the University of Houston and University of New South Wales. The two universities from the United States (Cornell University and the University of Houston) are focused on cryptography, network security, security of data, data privacy and smart contracts.

This plot indicates that universities from Asia have more interest to adopt blockchain in IoT research, compare to universities from the United States that have more concern in the

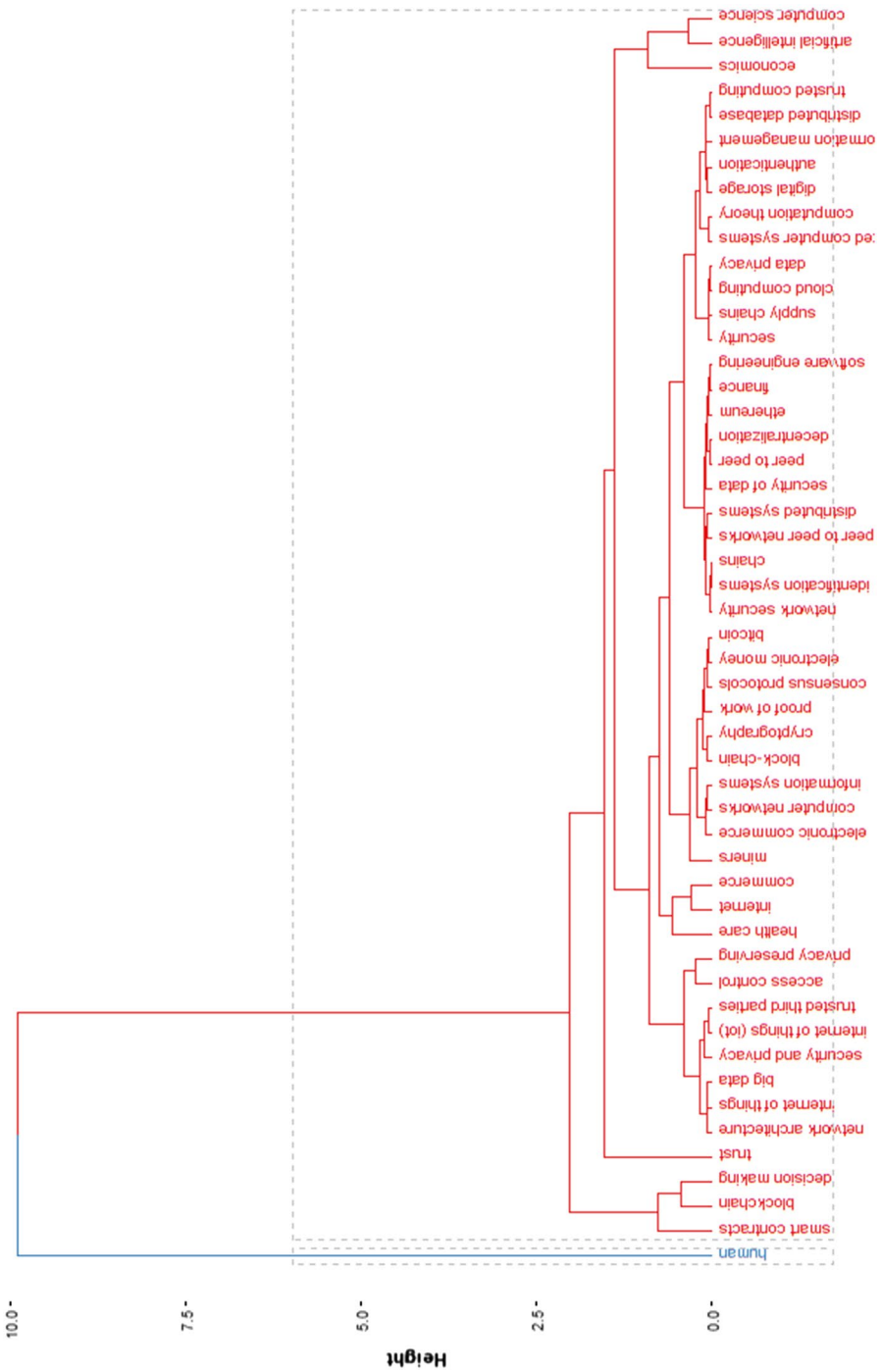

Fig. 8 Topic dendrogram

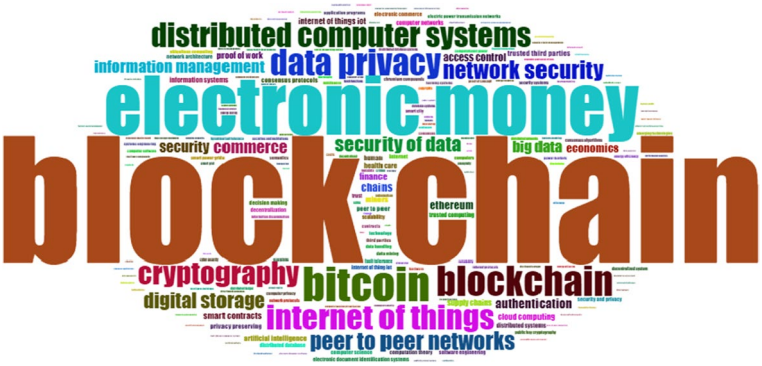

Fig. 9 Word cloud of blockchain keywords

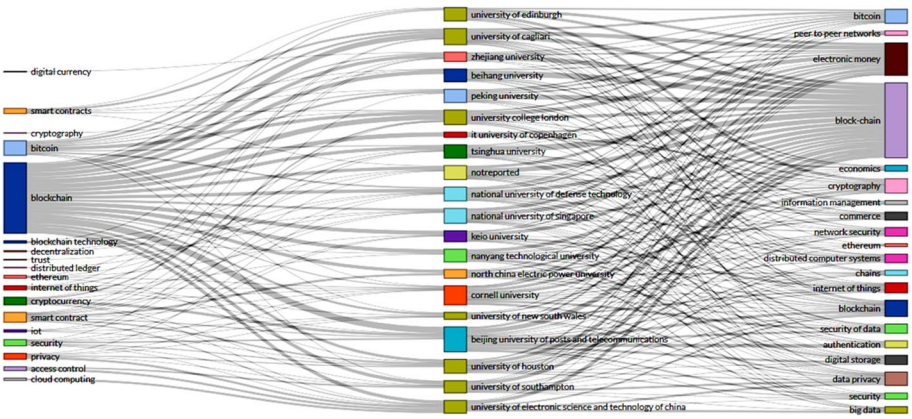

Fig. 10 Multi-fields plot between affiliation and keywords

security field. On the other hand, articles related to blockchain that receive attention and were cited by other researchers are discussed below.

Total citations

Table 8 tabulates the sources or journals that received a number of citation from other articles, placed within the top 20 rankings. This information noticed certain articles received many citations in certain years. This shows the trend that certain articles are worth referring to in specific years only. Many authors also combined blockchain technology with other areas, hence they only cited papers that were related to their research activities.

From another perspective, it was noted that certain blockchain papers were cited steadily in each year, such as ranking number one and ten (both published in 2013 and received citations in similar number in each year). This indicates that the papers are competent and they also cover the main information of the blockchain and are suitable for other researchers in their references.

Table 8 Articles that receive citations

Ranking no.	Authors with the source (top 20)	Total citation (number of citation received)	Total citation per year
1	Decker C; Wattenhofer R, (2013), Peer-to-Peer Computing (P2P), IEEE Thirteenth International Conference	92	18.4
2	Zyskind G; Nathan O; Pentland As, (2015), Proceedings of IEEE Security and Privacy Workshops	88	29.33
3	Christidis K; Devetsikiotis M, (2016), IEEE Access	81	40.5
4	Eyal I; Sirer Eg, (2014), Lecture Notes in Computer Science	79	19.75
5	Kosba A; Miller A; Shi E; Wen Z; Papamanthou C,(2016), Proceedings: 2012 IEEE Symposium on Security and Privacy	60	30
6	Luu L; Chu D-H; Olickel H; Saxena P; Hobor A, (2016), ACM Conference on Computer and Communications Security	43	21.5
7	Yuan Y; Wang F-Y, (2016), Zidonghua Xuebao/Acta Automatica Sinica	43	21.5
8	Tschorsch F; Scheuermann B,(2016), IEEE Communications Surveys & Tutorials	41	20.5
9	Gervais A; Karame Go; Wüst K; Glykantzis V; Ritzdorf H; Capkun S,(2016), ACM Conference on Computer and Communications Security	40	20
10	Moser M; Bohme R; Breuker D, (2013), eCrime Researchers Summit	40	8
11	Yli-Huumo J; Ko D;Choi S; Park S; Smolander K, (2016), Plos One	32	16
12	Zhang N; Wang Y; Kang C; Cheng J; He D,(2016), Zhongguo Dianji Gongcheng Xuebao/Proceedings of the Chinese Society of Electrical Engineering	29	14.5
13	Spagnuolo M; Maggi F;Zanero S, (2014), Lecture Notes in Computer Science	29	7.25
14	Azaria A; Ekblaw A; Vieira T; Lippman A,(2016), Proceedings of International Conference on Open and Big Data	28	14
15	Xu X; Pautasso C; Zhu L; Gramoli V; Ponomarev A; Tran Ab; Chen S, (2016), The Working IEEE/IFIP Conference on Software Architecture (WICSA)	27	13.5
16	Vukolic M,(2016), Lecture Notes in Computer Science	26	13
17	Croman K; Decker C; Eyal I; Gencer Ae; Juels A; Kosba A; Miller A; Saxena P; Shi E; Sirer Eg; Song D; Wattenhofer R,(2016), Lecture Notes in Computer Science	23	11.5
18	Iansiti M; Lakhani Kr,(2017), Harvard Business Review	21	21
19	Pilkington M, (2016), Research Handbook on Digital Transformations	21	10.5
20	Decker C; Wattenhofer R, (2015), Lecture Notes in Computer Science	21	7

In noting the highest source from the table, it is obvious that lecture notes in computer science (LNCS) comprise five jotted papers. This proves that this source provides most of the blockchain information, therefore, many authors refer to lecture notes in their citations. This source chooses and publishes the latest research in multiple areas of computer science in distinguished conferences, proceedings, and series. The LNCS has two subseries: (1) Lecture notes in artificial intelligence (LNAI); and (2) Lecture notes in bioinformatics (LNBI). The LNCS is indexed in digital bibliography & library project (DBLP), ISI conference proceedings citation index, Scopus, engineering index (EI), and Google scholar.

Besides the LNCS, there are more conference sources in the top 20 papers in the table. The top three were the IEEE Thirteenth International Conference, the IEEE Security and Privacy Workshops, and the IEEE Access. Most of these conferences require minimal time in their review process and they also require a low number of pages. In comparison, the journal review procedure of a worthy journal takes a longer time. This explains why many authors prefer to record their original ideas and research method in conferences before they continue to update their conference paper information to the journal level. By practicing this, they are able to preserve their novelty in their research, making other researchers unable to duplicate their ideas in blockchain technology. Besides conferences, there are also researchers who were interested in publishing blockchain studies in journals such as the Plos one and the IEEE access. The reason is that both are open access journals.

As seen in the table, the sources for articles that received citations encompass the IEEE Thirteenth international conference (row one), the IEEE security and privacy workshops (row two), the IEEE Access (row three), and the IEEE symposium on security and privacy (row five). These top five IEEE sources have outstanding citations of higher than 50 citations in total. This indicates that conferences attract more researchers to publish their blockchain research and the most highly cited conference source is the IEEE. Meanwhile, other than citation, the following section below discusses which country is involved in blockchain research.

Country

This section deliberates the countries that involved in blockchain research. It highlights the author's country that recorded in the publications. It comprises the country's total of articles, publications, total of citations, and collaboration network. The following sub-section begins with the country total of articles.

Country total of articles

Figure 11 visualizes the countries involved in blockchain research. The first ranking country is the United States with total articles of 103, China (71) and Germany (42). It is worth to mention that these three countries are located in different continents; (1) the United States represents North and south America; (2) China represents the best ranking country in Asia; and (3) Germany marks the highest publication among other countries in Europe. This information states that each continent has a leading country in blockchain research activities.

The figure also depicts that the blue color exists more in multiple countries in the Europe continent. This shows that the countries in Europe (United Kingdom, Germany, and Italy) adopted blockchain in their research paper more than other continents. Furthermore, more countries in Europe are attempt to involve in blockchain research as

Fig. 11 Total of articles in the country

many small blue colors exist surrounding the continents. This evidence shows that the number of blockchain researchers are increasing in Europe and would expect more publications in the near future.

Certain countries such as Kazakhstan, Mongolia, Algeria, and Venezuela were excluded. It is important to note that Venezuela is a country that currently faces an economic crisis and its money has less value. Therefore, they utilize cryptocurrency coin and currently practices blockchain in their daily lives. The digital cryptocurrency is referred to as petro (PTR) (Gusson 2018; Memoria 2019). The Venezuela government launched the PTR to overcome its economic crisis. As a result of this situation, universities in Venezuela were unable to join the blockchain research. Thus, Fig. 11 is unable to mark any publication in Venezuela.

Besides the Europe continent, Asia is also actively involved in blockchain research. As shown by the significant blue colors and a total number of articles; China, South Korea, Japan, and Australia are countries that lead in Asia continent. Compare to other countries on this continent, this figure indicates that these countries are able to discover the true potential of the blockchain and contributed their idea in publications.

Country publications

This section discusses the blockchain articles in terms of single and multiple publications for each country. It also aims to observe the collaboration network occurring in various countries in publishing blockchain articles. Table 9 shows that only certain countries published in their own country without collaborating with others, for instances, Canada, India, and Brazil. Almost all other countries prefer to publish in single articles, with only a few articles that are shared between countries. The table displays that the top three leading countries are the United States, China, and Germany.

Figure 12 provides the information in the graph for more illustrious and easier observations. It offers an insight into the information which encompasses both single country publications (SCP) and multiple country publications (MCP).

Table 9 Country with blockchain publications

Country (top 20)	Articles	SCP (single country publications)	MCP (multiple country publications)
United States	103	86	17
China	71	56	15
Germany	42	30	12
United Kingdom	38	30	8
Italy	31	21	10
Japan	31	27	4
Switzerland	31	24	7
Korea	29	26	3
Australia	26	20	6
France	17	11	6
Canada	16	16	0
India	16	16	0
Singapore	12	8	4
Austria	11	7	4
Taiwan	11	9	2
Spain	9	4	5
Netherlands	8	6	2
Brazil	7	7	0
Denmark	7	4	3
Estonia	6	3	3
Hong Kong	6	2	4

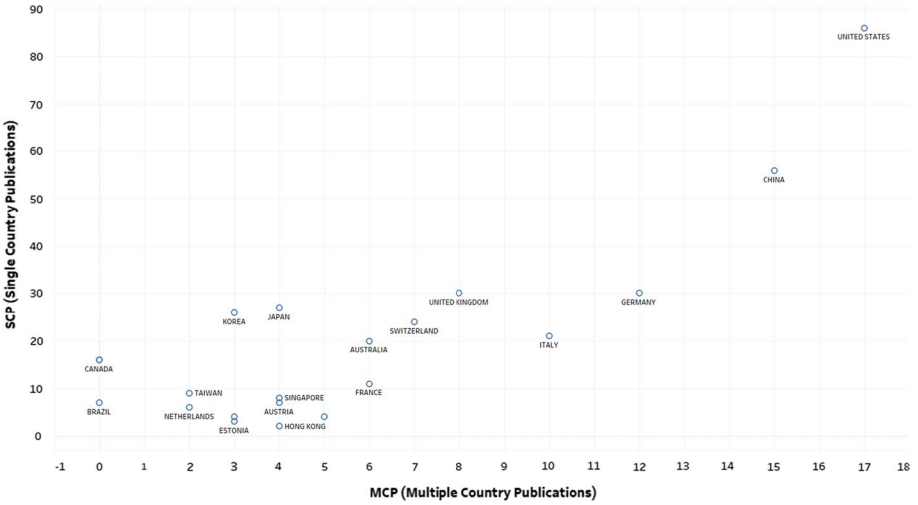

Fig. 12 Country with publications in figure form

In MCP and SCP points of view, Fig. 12 shows that the United States marked the highest spot, which indicates that this country actively published in both single and multiple publications, followed by China and Germany.

However, in the MCP perspective, the figure shows that several countries have less interest in publishing with other countries. These countries include Brazil and Canada which are marked with zero MCP. In contrast, they showed more interest in publishing in the SCP range as the publication values in the SCP were more than one. It is interesting to note that the highest values in the MCP were less than the SCP, which is 17 and 86 respectively. This trend proves that most countries are more interested in collaborating and publishing blockchain research in a single rather than multiple countries.

However, there is one country which chose to collaborate with other researchers. Hong Kong was noted to be the lowest among all countries in SCP, which published only two papers. Nevertheless, Hong Kong showed interest in joining and collaborating with other countries since it published four papers in the MCP region. This value demonstrates that Hong Kong is more comfortable to collaborate with other countries in blockchain publications.

Country collaboration map

Figure 13 depicts the country collaboration throughout the world with blue color indicates as there is collaboration exists in that country. The dark blue shows a higher frequency of collaboration with other countries. The countries that actively collaborate with other countries are United States, United Kingdom, German, Italy, France, China, and Australia. The map indicates that the United States is the country that collaborates most by engaging almost all active countries in publishing research in blockchain, followed by China and a few countries in Europe. It demonstrates that collaborations among countries will able to increase the amount of publications, compare to publications in a single country.

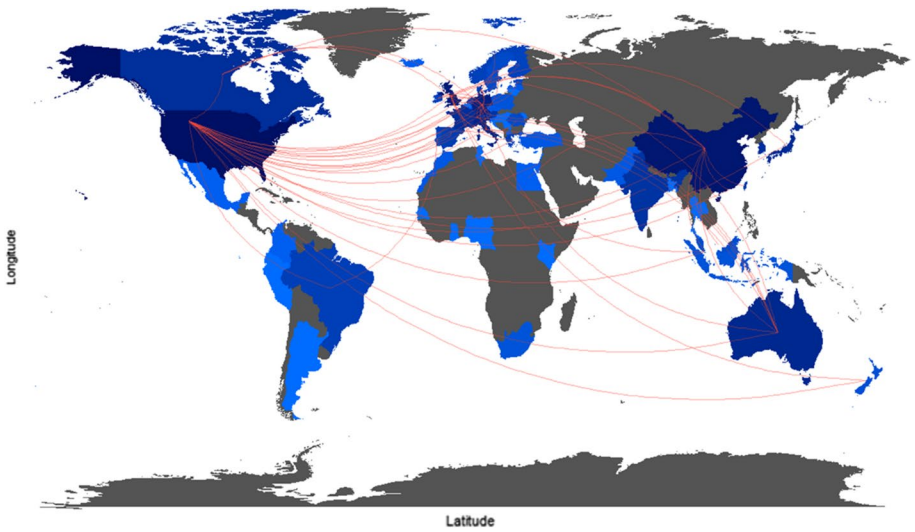

Fig. 13 Country collaboration map

Country total citations

This section reveals the blockchain publications which received citations from other researchers in the top 20 rankings, globally. Table 10 tabulates the total and average article citations values. It sorts by the total of citation from the highest to lowest. It lists the United States marked the top place followed by Germany and Switzerland.

Table 10 illustrates that certain countries received low total citations, but received high average article citations value. The involved countries are Finland (32–8), Singapore (71–5.9167), and Switzerland (149–4.8065). This evidence shows that these three countries published a low number of articles, however, received significant citations worldwide in each article. It also shows that these countries published a good research quality of blockchain articles rather than quantity.

However, Fig. 14 visualizes both total and average citations. It highlights the total citations with blue color and the average citations in circle form.

In comparison with the previous Sect. (4.4.2—country publication), Switzerland only published 31 articles but it received an outstanding citation of 149. It surpasses China which published a higher total of articles but received a lower citation score than Switzerland. This is similar to Singapore, which only published 12 articles but had received citations higher than the United Kingdom.

The information revealed that Switzerland and Singapore had published in high quality journals, thereby attracting other researchers to cite and refer. In the interest to

Table 10 Country with a total of citations

Country	Total citations	Average article citations
United States	326	3.165
Germany	160	3.8095
Switzerland	149	4.8065
China	128	1.8028
Singapore	71	5.9167
United Kingdom	63	1.6579
Japan	54	1.7419
Australia	50	1.9231
Italy	36	1.1613
Finland	32	8
Austria	22	2
Korea	21	0.7241
Estonia	15	2.5
Morocco	15	7.5
Denmark	13	1.8571
France	12	0.7059
Norway	12	2.4
Hong Kong	11	1.8333
Netherlands	11	1.375
Canada	10	0.625
New Zealand	6	3

Fig. 14 Country with total citations in the world map

discover the relationship between these countries, the following section provides network collaboration between countries, keywords, and affiliations.

Network

This section provides the bibliometric analysis of the blockchain in network form. It consists of country collaboration and keyword co-occurrences network. This network was constructed so as to be able to observe the movement of the different nodes that are connected to each other.

Country collaboration network

In the interest of detecting the countries that were actively collaborating with each other, Fig. 15 provides a record of networking circles of collaboration. Collaboration is a network that will indicate how the authors are linked to the network as a result of their co-authorships (Glänzel and Schubert 2004).

The colored circle noted in each node of the network, as shown in the figure, represents the total number of articles. The figure depicts that the USA is a country that collaborates most in publishing blockchain articles followed by China, the United Kingdom, German, Italy, and Switzerland. The figure also revealed that many lines are connected to each other in the upper part of the collaboration network. This reveals that the countries in the upper part were actively collaborating with each other when compared to countries in the lower part. Most of the countries in the upper part were from the Asian region, such as Malaysia, Singapore, China, Indonesia, New Zealand, Australia, India, Hong Kong, New Zealand, Japan, and Korea. This implies that countries in the Asian region preferred to collaborate with others when publishing articles in blockchain research activities, rather than publishing in a single country.

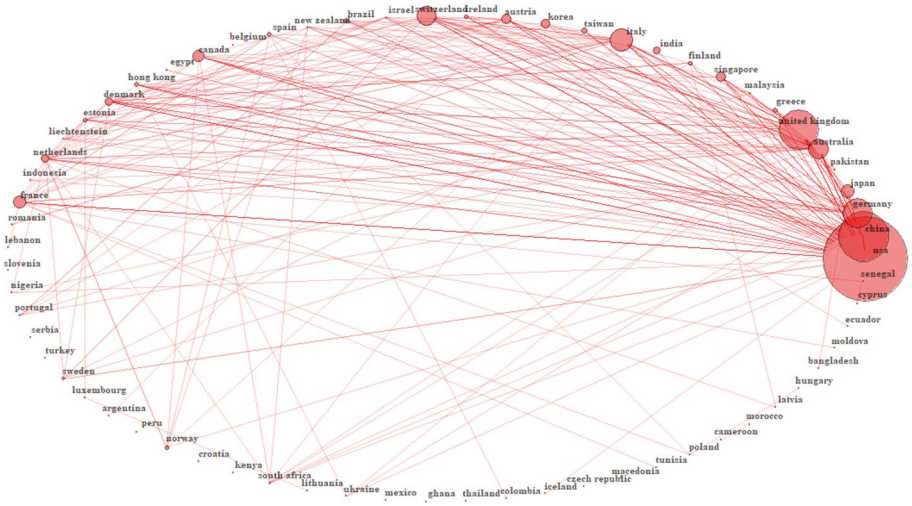

Fig. 15 Country collaboration layout network

Keyword co-occurrences network

Noted in the publications, it is crucial for each published article to include keywords after the abstract. These keywords consist of the research fields that were involved in the respective articles. Figure 16 provides the information to uncover which fields were related to blockchain research. It establishes the keyword co-occurrences of the network.

As shown in the figure, the authors include 'block-chain' as a keyword more than 'blockchain'. The reason is that in previous years, blockchain is a new term, therefore it was excluded in the global dictionary. Hence, there are differences in the keyword. Nonetheless, both terms refer to the same word, which is blockchain. The figure depicts that the researchers combine blockchain with multiple keywords, indicates that they combine blockchain with multiple areas of research. The common areas that combined with blockchain are electronic money, bitcoin, cryptography, and bitcoin.

Additionally, the most involved keywords, after blockchain, are electronic money, cryptography, data privacy, digital storage and internet of things. This information reveals that researchers conduct blockchain for electronic money as their first attempt. Subsequently, they would relate blockchain to other fields such as cryptography, data, and the internet of things (Husain et al. 2018; Cherian and Chatterjee 2019; Li and Shang 2019; Jennath et al. 2019).

The keyword co-occurrences network further recorded three different words in different capitalizations. The words include; (1) Internet of things (IoT). (2) Internet of thing (IoT). (3) Internet of things. To be precise, the researchers were referring to the same field, which is IoT. Previous section in this paper (4.3.2—Authors keywords) also witnesses a high demand of blockchain in the IoT field. This evidences provide information that the trend of combination between IoT and blockchain is outstanding and the amount of publication in these fields would be increase in the near future (Ryu et al. 2019; Chen et al. 2019; Casado-Vara et al. 2019; Roman and Ordieres-Mere 2019; Kim et al. 2019).

The analysis further showed that researchers also have the interest to combine blockchain with healthcare fields. This proves that blockchain has a competent security

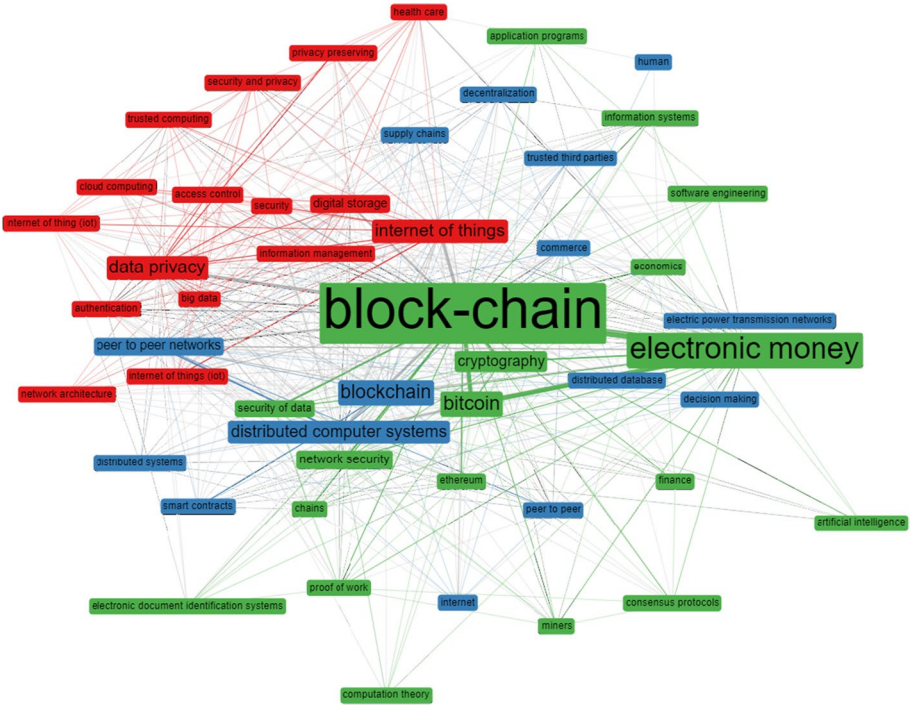

Fig. 16 Keyword co-occurrences network

structure and the security practitioners have confidence in using blockchain and able to improve and save human lives. Other than country and keyword network collaborations, the next section provides affiliation collaboration network to discover the collaboration between universities.

Affiliation collaboration network

The colored node in the network, as shown in Fig. 17, represents the collaboration of network between universities and colleagues from different countries. The University College London from the United Kingdom collaborates with the London School of Economics. While, the purple color node represent five institutes that have collaboration between Air Force Research Laboratory, Tennessee State University, Old Dominion University from the United States of America, Institute of Information Engineering and University of Chinese Academy of Sciences from China. The red color node represents the collaboration between the National University of Defense Technology, Qingdao Academy of Intelligent Industries from China and Institute of Automation from Jerman.

This figure reveals that the universities in China preferred to collaborate with their own country, compare to others. The reason is when referring to Sect. 4.3.2 (Author's keyword) and in addition with this figure, these demonstrate that they have the similar interest which is to explore the potential in IoT with blockchain research. In order to provide more information in a blockchain, the following section describes how it works and its utilization (Drosatos and Kaldoudi 2019; Estrada-Galinanes and Wac 2019; Lopes and Pereira 2019;

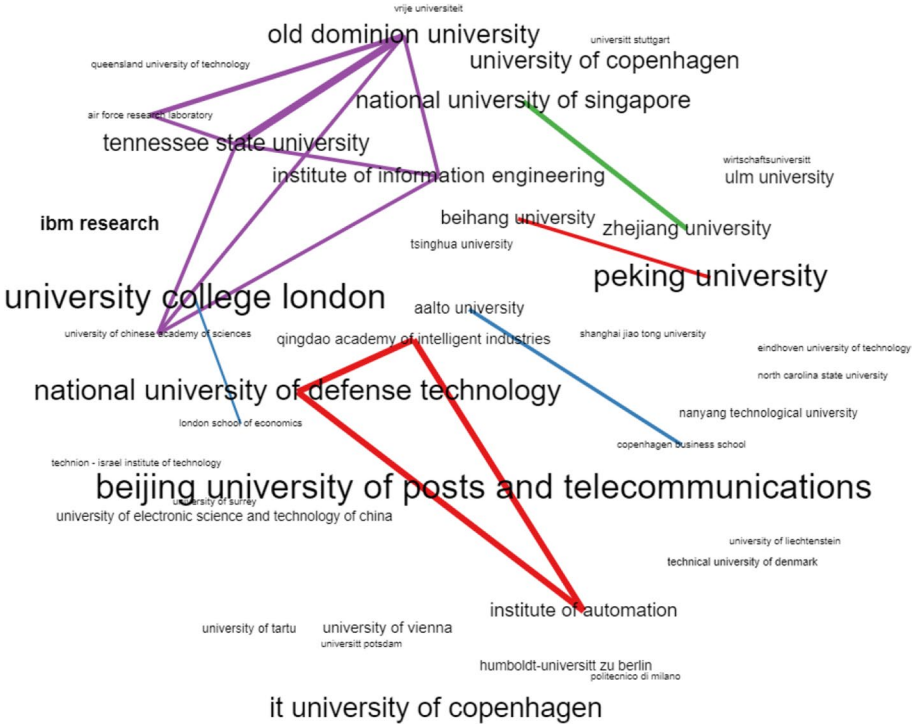

Fig. 17 Affiliation collaboration network

Dwivedi et al. 2019; Vazirani et al. 2018; Al Omar et al. 2019; Cao et al. 2019; Chen et al. 2019; Alonso et al. 2019).

Utilization of blockchain

In general, the most common attraction of the blockchain is cryptocurrency (digital money). Nevertheless, research analysts from the government sector, corporate organizations, security institution as well as industrial segment are able to extend the potential of blockchain and its interests well beyond the domain of cryptocurrencies. These domains using blockchains encompass the record transactions, smart contracts, and data purposes. Figure 18 illustrates these interests in chronological order.

Phase 1

As shown in the Fig. 18, phase one begins with a request to broadcast for peer-to-peer (P2P) network nodes in the blockchain network. This is the initial phase where the decentralization of authentication takes place. In cryptocurrency @ digital coin situation, when person A click the submit button to send bitcoin to person B, the request will start and proceed to phase two.

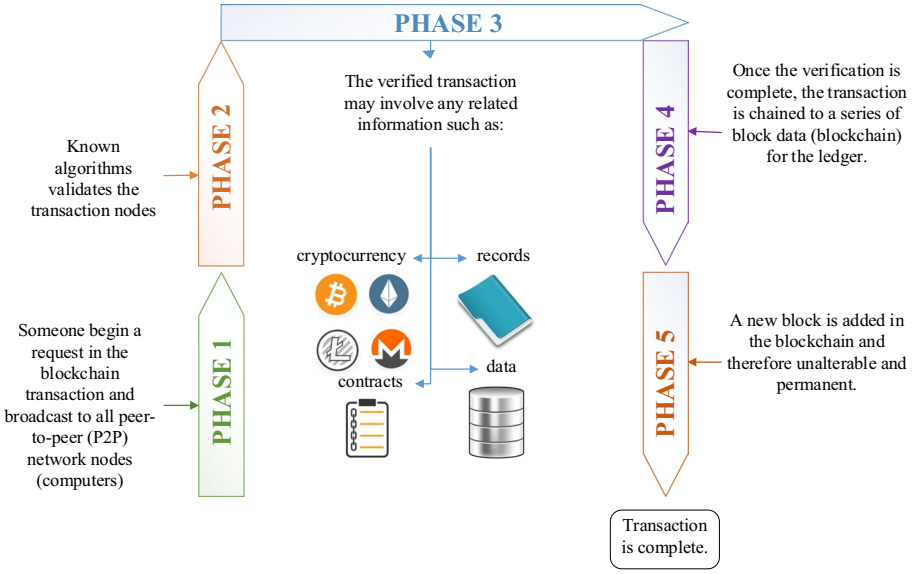

Fig. 18 How blockchain works

Phase 2

The following phase is where the algorithm is done to validate the transaction. In cryptocurrency example, it is important to validate each transaction to avoid any person to spend the digital coin twice or double-spending. Examples of the algorithms used are SHA-256, Blake, Crypto Night, and Equihash. Table 11 addresses Proof of work (PoW) algorithm for each digital coin. These validation algorithms also are known as a consensus algorithm. Section 6 discusses this information in detail.

On the other hand, another situation in the blockchain network, such as property matters (land, car, and house), the blockchain developer may use other than validation algorithm. Instead, they would apply lawyer approval to validate each transaction either legal or illegal. If the lawyer disapproves it, this process will unable to proceed to the next phase. However, if the lawyer checks all the requirements and approve, the following phase (phase three) will initiates.

Table 11 Cryptocurrency and its PoW algorithm

Cryptocurrency	Algorithm
Bitcoin (btc) Bitcoin cash (bch)	Secure hash algorithm (SHA-256)
Ethereum (eth)	Ethash
Litecoin (ltc)	Scrypt
Dash (dash)	X11
Zcash (zec)	Equihash
Monero (xmr)	CryptoNightR

Phase 3

Phase three is where the blockchain involves the interest elements (cryptocurrency, records, contracts, and data). Table 12 tabulates the different situations with different interest elements that store in each block in the blockchain network. In cryptocurrency situation, each block may involve information such as the timestamp of the transaction and amount of coin spent, Meanwhile, in records example, each block may keep the information of the person that enter and leave the vault room. While the contract situation, each block saves the information between the private sector and government contract. While for the data example, each block will save the weather data that collected from the weather sensor. This situation will fall in the IoT area, which many researchers have many interest on this as explained in previous section (Sect. 4.3.2). Once phase three is done, the following step is the phase four.

Phase 4

In phase four, this is where the blockchain network store and begin to chain the data together with the previous block. Once it chained, any user is unable to tamper or change the data. If any situation needs to change the information on the block, therefore the user needs to create another block as usual process similar to phase one. Then, the new block needs to mention that there is a correction in the respective block and the update information is provided in this new block.

All the information in all the blocks are available in block explorer. It considers as public ledger for public reference and this record is permanent. The ledger is then distributed to all the participants in the blockchain network and all the computers (nodes) in this network have similar data. It is because the blockchain used P2P features which adopt decentralized databases. With these features, it is good for security because if one computer (server) is attacked, other computers have the backup data. For instance, in cryptocurrency data example, Table 13 tabulates the transaction of the digital coin in different websites with different servers installed, but once it participated in the similar blockchain network, they provide the equivalent data information on-the-fly (live). Each website will provide the same current block, for example, block 712562. After another transaction is done, the block will increase one block, and the latest bock will turn to 712563. And all the website will provide the latest block which is 712563.

Phase 5

In phase five, all the information in the blockchain continues to increase from time to time depends on the activities. If there is no activity, the number of the block will still remain

Table 12 Interest elements saved in a block according to certain situations

Situations	Example of interest elements to store in each block
Cryptocurrency	Timestamp and amount of coin (date, price)
Records	Vault records information (staff number, date, time)
Contracts	Government contracts information (time, meeting location, agreement information)
Data	Weather sensors data (temperature, humidity)

Table 13 Each cryptocurrency with its block explorer

Cryptocurrency	Block explorer link
Bitcoin	https://blockexplorer.com/
	https://live.blockcypher.com/btc/
	https://btc.com/
Bitcoin cash	https://bch.btc.com/
	https://blockchair.com/bitcoin-cash/blocks
	https://blockdozer.com/
Ethereum	https://etherscan.io/
	https://blockscout.com/eth/mainnet/
	https://blockchair.com/ethereum

without addition. The data in it is constantly updated and all the computers have the latest copy of the data (Marsal-Llacuna 2017). Therefore, the history of the data is all available from the first block until the latest block. This is useful for audit and monitoring the activities. Hence, blockchain is useful in many areas such as IoT, property records and vote system.

Consensus algorithm

In order to update the ledger, the blockchain network needs to achieve a consensus by utilizing an algorithm. From the cryptocurrency point of view, all the participants in the distributed network need to agree to the consensus. This is to avoid any double-spending on the value. Agreeing with the consensus means that in the blockchain distributed network, it is indicated that every participant agrees on the latest status in the ledger (current money value in every account) and every one of them confirms that there is no double-spending happening.

In other words, the consensus is a favored word that signifies "general agreement" which is an imperative part of blockchain innovation. Rather than having a specialist to keep accounts and bringing the things together in a single element, similar to a bank or concentrated online payment framework, the digital currency utilizes appropriated records or blockchain to record data. In this way, the blockchain system needs the general agreement to record data such as the balance accounts of each address, exchanges, and transaction activities. All the consensus algorithm mechanisms intend to secure the system by making it costly to assault the system and more gainful to help secure it (Li et al. 2017). In Fig. 19, there are five types of consensus algorithms (Mingxiao et al. 2017): (1) proof of work (PoW), (2) proof of stake (PoS), (3) byzantine fault tolerance (BFT), (4) proof of elapsed time (PoET), (5) proof of bandwidth (PoB) and (6) proof of authentication (PoAh). Table 14 summarizes and differentiate between all these algorithms.

Proof of work (PoW)

Proof of work (PoW) is one of the consensus algorithms that solves the mathematical algorithms by guessing the answer. The computer that has high computational power will have faster guessing and high possibility to guess the right answer. Then, the person who owns that computer will receive an amount of money in digital currency as a reward.

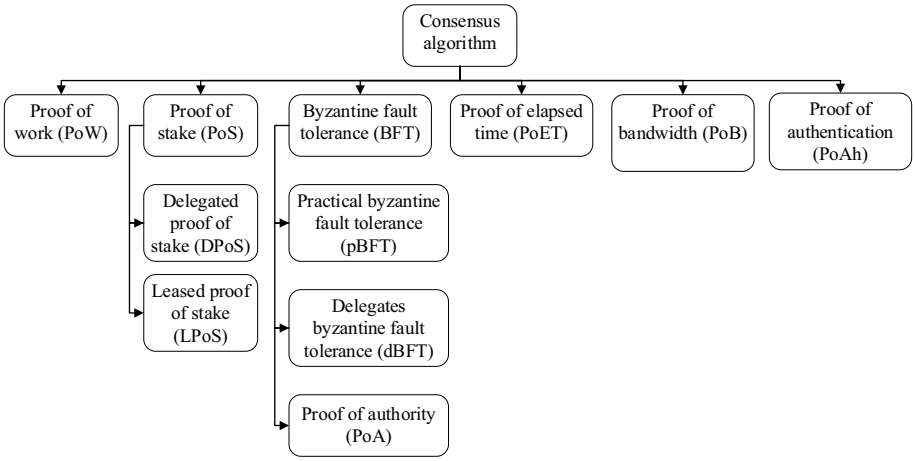

Fig. 19 Taxonomy of the consensus algorithm

Searching for an answer to the mathematical problem is similarly like a game, essentially an amusement. Whoever initially finds the answer derived from the consensus algorithm will be the first to be rewarded.

In PoW, the miners are unable to hack the system as they apply the real physical resources to solve the algorithm problems. The examples of the real physical system are graphical processing unit (GPU) and application-specific integrated circuit (ASIC) machine (Bitmain 2019). These machines consume a high amount of electricity and energy. From an ecological point of view, this is not ideal as it causes the miners to have high energy costs while also being harmful to the environment unless renewable sources are used. The fact is that it requires a considerable amount of computing power which is more than what the average person is able to afford. Hence, the researchers invented an alternative known as the green consensus algorithm, called the proof of stake (PoS), to overcome these problems.

Proof of stake (POS)

Similar in objective to the PoW, the PoS is a method to validate the blockchain transactions. However, the difference is PoS use coins instead of computational power. PoS algorithm executes its method by allocating the miner coins on a block in order to validate the transaction. The algorithm chooses the miners according to the number of the miner's coin which they just allocated and for the duration they hold. The miners simply need to demonstrate that they have a specific level for every accessible digital coin. Then, they will receive rewards. This PoS method would be faster and more productive than the PoW framework. Due to the fact that anyone can become a miner, the PoS method also offers a straight scale with regards to the level of the block which a miner can affirm on the grounds that it depends on the digital coin owned. For instance, Ethereum decided to change from the PoW to the PoS framework to affirm transactions because of the PoS advantages. Other than the PoW and PoS, researchers have also constructed the practical byzantine fault tolerance (pBFT) as an another alternative method.

Table 14 Differences between consensus algorithm

	PoW	PoS	BFT	PoET	PoB	PoAh
Based on	Mining	staking coin	Exchange message between untrusted parties	Lottery system	Bandwidth	Authentication
More information	The person that solves the mathematical equation first will get the coin as rewards	The person that own big amount of coin will validate the transaction	Achieve consensus among multiple parties without trust each other	Where each and every node is similarly likely to be a winner	Contributing the bandwidth capacity to verify the system	Achieve authentication from its source and who authenticate the block first
Energy consumption	High	Low	Depends on the activities	Low	Depends on the activities	Low

Delegated proof of stake

Designated proof-of-stake (DPoS) is much more advanced than the PoS system. The DPoS utilizes a notoriety framework and real-time voting to accomplish the agreement. The participants vote for super representatives to secure their system and the DPoS will reward the super representatives by validating exchanges for the following block. As such, in the tron (TRX) digital coin example, there will be a decision to pick 27 super representatives with a yearly reward pool of 1,009,152,000 TRX (Tron Live 2018). The primary difference between the DPoS and PoS is that the participants in the former network have more governance rights in the system.

Since the vote in the DPoS is continuous and on-going, it is observed that if the super representatives act badly or perform an unscrupulous act, the community in the network will be able to expel their votes, basically terminating the bad representatives. The super representatives should attempt their best to comply with all obligations and to keep the system up as high as conceivable. Otherwise, the community or participants in the network may reject the super representatives. The advantages of the DPoS are its decentralized convention that is vote based, its self-governing participants in the network, the free elections, and its general legitimacy.

Leased proof of stake (LPoS)

In the general viewpoint of the PoS, the participants in the network who keep and hold small balances are excluded from staking a block. This is because it would consume years to generate a block which also depends on luck situations. This implies that the holders with low balance were excluded from running a node; they are left to keep the system up to a higher balance as owned by bigger players. Therefore, this is where the LPoS advantage come in.

Since network security is much better when there are more participants, the LPoS considers these little holders who join in running a node together with the bigger holders. The LPoS accomplishes its mechanism by enabling holders to rent or lease their balances in order to join the network in staking the nodes. The leased funds stay in the full control of the holders. They are able to move or invest any time according to their needs or until the lease point ends. Leased coins increase the 'weight' of the staking node, expanding its chances of being included and being allowed to add a block of the transaction. The LPoS will then reward the leasers by dividing the amount of the lease proportionally.

Byzantine fault tolerance (BFT)

The BFT is based on the Byzantine's generals case in a war. It gathers the respective generals who wish to achieve an agreement in attacking the country. Therefore, they need to choose either to commence an attack or to withdraw. Depending on the situation and experience of each general, some may prefer to assault, while others may prefer to withdraw. This is a crucial decision as the war could turn into a defeat and become more terrible than when it suffers an organized assault or through a planned withdrawal. Many researchers mentioned this algorithm in software-defined network research (Yuan et al. 2018). Due to the advantages offered by these Byzantine war case, crypto researchers began adopting it

in blockchain research as another consensus algorithm, for example, practical byzantine fault tolerance (PBFT) and delegated byzantine fault tolerance (DBFT), to aid in validating transactions (Gramoli 2017).

Practical byzantine fault tolerance (PBFT)

In 1999, Miguel Castro and Barbara Liskov introduced the practical byzantine fault tolerance (PBFT) as improvements in optimizing research (Castro and Liskov 1999). It was used to improve the original byzantine fault tolerance (BFT) mechanism. The algorithm works in asynchronous systems which are similar to the Internet mechanism which combines the imperative optimizations that enable it to perform proficiently. The algorithm adopts an efficient authentication scheme which is public-key cryptography, based on message authentication codes during the normal operation. This type of cryptography is able to avoid latency and throughput bottleneck.

Delegated byzantine fault tolerance (DBFT)

The delegated byzantine fault tolerance (DBFT) consensus algorithm acknowledges two kinds of participants in the blockchain system: (1) Professional node operators (execute nodes as a source of income); and (2) Participants who are interested in accessing blockchain advantages. Consequently, this algorithm verifies the block transaction by running through a consensus game held with specialized bookkeeping nodes, which constructs the delegated voting process. In the first step of the verification, the algorithm pseudo-randomly appoints the bookkeeping nodes. This is a kind of version that broadcasts to the rest of the network. If 2/3 of the remaining nodes agree with this kind of version, the DBFT will consider it as secure and the blockchain system will proceed to the next step. If less than 2/3 of the network agree, a different node is appointed to broadcast its version of the truth to the rest of the system, and so forth until the algorithm finishes establishing the consensus process.

By implementing this kind of consensus algorithm, it is impossible for any system to attack unless a majority of the network agree in committing financial suicide. The system is fork proof, and at every given moment, only one version of the truth exists. Without complicated cryptographic puzzles to solve, the nodes operate much faster and are able to compete with centralized transaction methods.

Proof of authority (PoA)

The proof of authority (PoA) (De Angelis et al. 2018) is another group of BFT consensus algorithm which has drawn the researcher's responsiveness due to its advantages of execution and toleration to faults. Parity (Authors 2018) and Geth (Authors 2018) are the two well-organized customers for permission setting of Ethereum that currently utilizes the PoA. In particular, the calculation of the algorithms works in rounds during which an elected party acts as the mining leader. The leader is responsible for proposing a new block to achieve a distributed consensus. Unlike the PBFT, the PoA requires fewer message trades hence, it gives better executions. Nevertheless, the real outcome of such execution change is quite hazy, as far as accessibility and consistency are concerned in ensuring a reasonable long-run synchronous system model.

Proof of elapsed time (PoET)

The proof of elapsed time (PoET) is also one of the consensus algorithms that avoid high resource utilization and high energy consumption. This is done by implementing a fair lottery system. It completes the consensus of each potential validator node that demands a secure random, holding up time from a trusted execution condition which is already implemented into the computing platform, such as Intel's SGX.

Intel, the renowned chip producing giant, developed the PoET idea in early 2016. It offers a readymade innovative instrument to solve the computing issue of "random leader election". Intel SGX is specific hardware equipment that is able to create a verification that was set up accurately in a secure area. For instance, if an outsider party uses the verification to verify or check whether the correct code is operating in the correct way, the system allows the network participants to demonstrate to different participants that it is operating the right trusted code for the network. Without this method, it will be difficult for the network to discover that the participant is truly operating the PoET's trusted code. Furthermore, the trusted code keeps on operating in a private environment which forbids any other application to investigate or inspect the memory space of the trusted code. This is to guarantees that any unscrupulous participant will be unable to cheat and control the PoET's trusted code after it has been set up.

In other words, the PoET is a permission type of blockchain. If this system wishes to join the network, any forthcoming networking participant must identify him/herself first. In view of the standard of a reasonable lottery system, where each and every node is similarly likely to be a winner, the POET system depends on spreading the odds of winning fairly, over the largest possible number of network participants.

This is achieved by considering the node of the network participant who waits randomly at a certain period of time. The first to finish the assigned waiting time wins the new block in the blockchain. Once the node in the network generates a random waiting time, it rests for that predetermined term. The node that wakes up first is the one with the shortest waiting time. It then commits a new block and it broadcasts the necessary information to the entire peer distributed network. The procedure is similarly repeated until the disclosure of the following block. The PoET needs to consider two important factors; (1) The network participant nodes which truly selects a random number and not a shorter length, picked intentionally by the participant in order to reach a goal to win and (2) The winner has truly finished the waiting time.

Basically, the work process is similar to the PoW calculation, but it is without its power utilization. Rather than being resource intensive, it enables the miners' processors to rest and change to different tasks for a certain time thereby, increasing its effectiveness.

Proof of bandwidth (PoB)

Unlike the Bitcoin PoW algorithm, the PoB confirms a verification by depending on the bandwidth instead of calculation. For instance, in the case of TorCoin (Ghosh et al. 2014), to mine this coin, a relay transfers the bandwidth capacity over the Tor network. Since relays are able to sell TorCoin for any existing type of coin, the TorCoin can successfully remunerate them for contributing the bandwidth capacity to the system, and clients are not required to pay for the access.

The TorCoin architecture comprises two types of protocol, the TorCoin, and TorPath. The TorCoin protocol is a Bitcoin variant that mines coins while the TorPath protocol assigns a circuit that consists of three passages: (1) Passage, (2) Center, and (3) Leave servers. The TorPath assigns these passages to every customer to approve the TorCoin minting through verifiable proofs of the bandwidth.

Proof of authentication (PoAh)

Proof of authentication (PoAh), is a consensus algorithm that implements a lightweight process that PoW (Puthal and Mohanty 2019). In order to achieve that, it consists of two types of authentication; 1) authenticate the block including its source; and 2) increasing a special value called as trust value, by adding one value to those that authenticate the block first. They also claimed that, in comparison with PoS, PoW, and PoA, it has low energy consumption, low computing, low latency, and low search space. This algorithm is created to suit the main problem of IoT technologies that frequently need low requirements for long-lasting operation.

Conclusion

Blockchain is an invention in Bitcoin digital currency and has been received many attentions from blockchain researchers globally. They are able to bring blockchain to higher levels and adopt it to solve problems in multiple areas. However, there are still lacks bibliometric reports exhibiting the exploration of an in-depth research pattern in this area. This paper has conducted a bibliometric analysis of the blockchain which involves 1119 articles that were published between 2013 and 2018.

This bibliometric analysis discovers that blockchain researchers were most interested to publish in conference rather than journal or in book form. The reasons are; (1) They would like to publish their genuine idea that involves blockchain, (2) To get feedback from the audience, and (3) To upgrade their conference paper to journal form.

Apart from that, the top author who published most is Xiwei Xu with 11 articles, followed by Ingo. M Weber with nine articles. They are the research members in a similar place (Data61, CSIRO, Sydney, Australia) and therefore easier for them to collaborate and published articles together. Their interest areas are to combine blockchain in IoT and business field. However, they are more involved as multi author compare to main.

Meanwhile, in dominance ranking, the top two rankings are Pass Rafael (main author—six articles) and Decker Christian (main author—four articles). Pass Rafael is a researcher in Massachusetts Institute of Technology (MIT) that have an interest in cryptography, which is a backbone in the blockchain. While Decker Christian is an author from ETH Zurich, Switzerland that concentrates on bitcoin, which is a first cryptocurrency that adopts blockchain.

On the other hand, in blockchain keywords, blockchain analysts are more keen to adopt blockchain in the Internet of Things (IoT). Before blockchain have been introduced, IoT receives many security issues to secure data among sensors. Meanwhile, after the researchers realized the potential of blockchain, they begin to adopt blockchain in IoT to overcome it. This evidence shows that blockchain will bring IoT to a higher level and contribute to more papers published in the near future.

Apart from IoT, they also apply blockchain in the healthcare research field, which involves human lives. Among all methods, blockchain receives outstanding attention from researchers to improve in medical and healthcare research interest. A topic dendrogram in Fig. 8 shows that they combine healthcare with internet and commerce. It demonstrates that the researchers are using blockchain to store healthcare data online, and gain profit with it.

In addition, this paper also discovers that blockchain researchers were adopting blockchain in data research field such as (1) data privacy; (2) digital storage; (3) security of data; (4) big data; and (5) distributed database. This proves that blockchain is able to secure data digitally and make it available online without limitation of size. This is also a reason that blockchain practitioners adopt blockchain to secure data in IoT and healthcare.

In-country point of view, the top three countries that published more papers in blockchain research are the United States, China, and Germany. This study also revealed that the number of blockchain researchers are increasing in Europe and would expect more publications in the near future. This is because many countries surrounding this continent are actively participating in blockchain research. It also appears that countries in Asia expectedly would participate together in this research. Furthermore, blockchain practitioners in Asia are more interested to combine blockchain with IoT, while the United States is more interested in securing data with blockchain.

This study also highlighted the utilization and consensus of the algorithm in blockchain research. It reviewed the potentials of blockchain which could be expanded to other areas other than digital currency only.

Acknowledgements This work was funded by Universiti Malaysia Pahang, under the Grant Faculty of Computer Systems and Software Engineering (FSK1000), RDU180361.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

Adewole, K. S., Anuar, N. B., Kamsin, A., Varathan, K. D., & Razak, S. A. (2017). Malicious accounts: Dark of the social networks. *Journal of Network and Computer Applications, 79,* 41–67.

Ahmed, H. A. S., & Zolkipli, M. F. (2016). Data security issues in cloud computing: Review. *International Journal of Software Engineering and Computer Systems (IJSECS), 2*(February), 58–65.

Al Omar, A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., & Rahman, M. S. (2019). Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Generation Computer Systems, 95,* 511–521.

Alonso, S. G., Arambarri, J., López-Coronado, M., & de la Torre Díez, I. (2019). Proposing new blockchain challenges in eHealth. *Journal of Medical Systems, 43*(3), 64.

Aniello, L., Baldoni, R., Gaetani, E., Lombardi, F., Margheri, A., & Sassone, V. (2017). A prototype evaluation of a tamper-resistant high performance blockchain-based transaction log for a distributed database. In *13th European dependable computing conference, (EDCC)*, pp. 151–154. Campus Biotech-Geneva, Switzerland.

Arfaoui, A., Ibrahimi, K., & Trabelsi, F. (2019). Biochar application to soil under arid conditions: A bibliometric study of research status and trends. *Arabian Journal of Geosciences*. https://doi.org/10.1007/s12517-018-4166-2.

Aria, M., & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics, 11*(4), 959–975.

Authors, P. (2018). "Parity" (Online). Available at https://www.parity.io/. Accessed July 25, 2018.

Authors, G. E. (2018). "Go Ethereum" (Online). Available at https://geth.ethereum.org. Accessed July 25, 2018.
Bartoletti, M., Bellomy, B., & Pompianu, L. (2019). A journey into bitcoin metadata. *Journal of Grid Computing, 17,* 3–22.
Bitmain (2019). "Bitmain" (Online). Available at https://shop.bitmain.com/?lang=en. Accessed May 06, 2019.
Brito, J., Nassis, G. P., Seabra, A. T., & Figueiredo, P. (2018). Top 50 most-cited articles in medicine and science in football. *BMJ Open Sport and Exercise Medicine, 4*(1), 1–8.
Cao, S., Zhang, G., Liu, P., Zhang, X., & Neri, F. (2019). Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. *Information Sciences, 485,* 427–440.
Casado-Vara, R., Chamoso, P., De la Prieta, F., Prieto, J., & Corchado, J. M. (2019). Non-linear adaptive closed-loop control system for improved efficiency in IoT-blockchain management. *Information Fusion, 49,* 227–239.
Castro, M., & Liskov, B. (1999). Practical byzantine fault tolerance. In *Proceedings of the third symposium on operating systems design and implementation* (pp. 1–14).
Chen, H. C., Irawan, B., & Shae, Z. Y. (2019a). A cooperative evaluation approach based on blockchain technology for IoT application. *Advances in Intelligent Systems and Computing, 773,* 913–921.
Chen, L., Lee, W. K., Chang, C. C., Choo, K. K. R., & Zhang, N. (2019b). Blockchain based searchable encryption for electronic health record sharing. *Future Generation Computer Systems, 95,* 420–429.
Cherian, M., & Chatterjee, M. (2019). Survey of security threats in iot and emerging countermeasures. In *6th international symposium on security in computing and communications, (SSCC)*, (Vol. 969, pp. 591–604). Bangalore, India.
Christian, D. (2019). Decker Christian (Online). Available at https://disco.ethz.ch/alumni/cdecker. Accessed May 15, 2019.
Cirillo, A., Mussolino, D., Saggese, S., & Sarto, F. (2018). Looking at the IPO from the 'top floor': A literature review. *Journal of Management and Governance, 22*(3), 661–688.
da Silva Filho, A. C., Maganini, N. D., & de Almeida, E. F. (2018). Multifractal analysis of bitcoin market. *Physica A: Statistical Mechanics and its Applications, 512,* 954–967.
De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain. In *CEUR workshop proceedings* (pp. 1–11).
Dehdarirad, T., Villarroya, A., & Barrios, M. (2015). Research on women in science and higher education: A bibliometric analysis. *Scientometrics, 103*(3), 795–812.
Dennis, R., & Disso, J. P. (2019). An analysis into the scalability of bitcoin and ethereum. *Advances in Intelligent Systems and Computing, 797,* 619–627.
Docampo, D., & Cram, L. (2019). Highly cited researchers: A moving target. *Scientometrics, 118*(3), 1011–1025.
Drosatos, G., & Kaldoudi, E. (2019). Blockchain applications in the Biomedical Domain: A Scoping Review. *Computational and Structural Biotechnology Journal, 17,* 229–240.
Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. *Sensors (Switzerland), 19*(2), 1–17.
Elango, B., & Rajendran, P. (2012). Authorship trends and collaboration pattern in the marine sciences literature : A scientometric study. *International Journal of Information Dissemination and Technology, 2*(3), 166–169.
Essaid, M., Kim, H. W., Guil Park, W., Lee, K. Y., Jin Park, S., & Ju, H. T. (2018). Network usage of bitcoin full node. In *9th international conference on information and communication technology convergence: Ict convergence powered by smart intelligence (ICTC)* (pp. 1286–1291). Maison Glad JejuJeju Island, South Korea.
Estrada-Galinanes, V., & Wac, K. (2019). Visions and challenges in managing and preserving data to measure quality of life. In *IEEE 3rd international workshops on foundations and applications of self systems (FASW)* (pp. 92–99). Torento, Italy.
Fahimnia, B., Sarkis, J., & Davarzani, H. (2015). Green supply chain management: A review and bibliometric analysis. *International Journal of Production Economics, 162,* 101–114.
Feizollah, A., Anuar, N. B., Salleh, R., & Wahab, A. W. A. (2015). A review on feature selection in mobile malware detection. *Digital Investigation, 13,* 22–37.
Firdaus, A., & Anuar, N. B. (2015). Root-exploit malware detection using static analysis and machine learning. In *Proceedings of the fourth international conference on computer science & computational mathematics (ICCSCM 2015)* (pp. 177–183). Langkawi, Malaysia.

Firdaus, A., Anuar, N. B., Karim, A., & Razak, M. F. A. (2017a). Discovering optimal features using static analysis and genetic search based method for android malware detection. *Frontiers of Information Technology & Electronic Engineering, 19,* 1–27.

Firdaus, A., Anuar, N. B., Razak, M. F. A., Hashem, I. A. T., Bachok, S., & Sangaiah, A. K. (2018). Root exploit detection and features optimization: Mobile device and blockchain based medical data management. *Journal of Medical Systems*. https://doi.org/10.1007/s10916-018-0966-x.

Firdaus, A., Anuar, N. B., Razak, M. F. A., & Sangaiah, A. K. (2017b). Bio-inspired computational paradigm for feature investigation and malware detection: Interactive analytics. *Multimedia Tools and Applications, 77*(14), 17519–17555.

Garcia-Alfaro, J., Navarro-Arribas, G., Hartenstein, H., & Herrera-Joancomartí, J. (2017). *Data privacy management, cryptocurrencies and blockchain technology* (pp. 1–446).

Ghosh, M., Richardson, M., Ford, B., & Jansen, R. (2014). A TorPath to TorCoin: Proof-of-bandwidth altcoins for compensating relays. In *7th workshop on hot topics in privacy enhancing technologies (HotPETs)* (pp. 1–13).

Glänzel, W., & Schubert, A. (2004). Analyzing scientific networks through co-authorship. *Handbook of Quantitative Science and Technology Research* (pp. 257–276). Dordrecht: Springer.

Governatori, G., Idelberger, F., Milosevic, Z., Riveret, R., Sartor, G., & Xu, X. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artificial Intelligence and Law, 26*(4), 377–409.

Gramoli, V. (2017). From blockchain consensus back to byzantine consensus. *Future Generation Computer Systems* (pp. 1–10).

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of Medical Systems, 42*(7), 130.

Gusson, C. (2018). Venezuelan Cryptocurrency Petro receives the Satoshi Nakamoto Prize in Russia (Online). Available at https://www.ccn.com/el-petro-the-venezuelan-cryptocurrency-receives-the-satoshi-nakamoto-prize-in-russia/. Accessed June 12 2018.

Han, R., Gramoli, V., & Xu, H. (2018). Evaluating blockchains for IoT. In *9th IFIP international conference on new technologies, mobility and security, NTMS* (pp. 1–5). Paris, France.

Hazim, M., Anuar, N. B., Ab Razak, M. F., & Abdullah, N. A. (2018). Detecting opinion spams through supervised boosting approach. *PLoS ONE, 13*(6), 1–23.

Hellani, H., Samhat, A. E., Chamoun, M., El Ghor, H., & Serhrouchni, A. (2018). On blockchain technology: Overview of bitcoin and future insights. In *IEEE international multidisciplinary conference on engineering technology (IMCET)* (pp. 1–8).

Hughes, A., Park, A., Kietzmann, J., & Archer-Brown, C. (2019). Beyond bitcoin: What blockchain and distributed ledger technologies mean for firms. *Business Horizons, 62,* 1–9.

Husain, Z., Suliman, A., Salah, K., Abououf, M., & Alblooshi, M. (2018). Monetization of IoT data using smart contracts. *IET Networks, 8*(1), 32–37.

Iefremova, O., Wais, K., & Kozak, M. (2018). Biographical articles in scientific literature: Analysis of articles indexed in web of science. *Scientometrics, 117*(3), 1695–1719.

Jennath, H. S., Adarsh, S., & Anoop, V. S. (2019). Distributed IoT and applications: A Survey. In *Studies in computational intelligence* (Vol. 771, pp. 333–341). Springer, Singapore.

Juhász, P. L., Stéger, J., Kondor, D., & Vattay, G. (2018). A Bayesian approach to identify bitcoin users. *PLoS ONE, 13*(12), 1–21.

Kim, S.-K., Kim, U.-M., & Huh, J.-H. (2019). A study on improvement of blockchain application to overcome vulnerability of IoT multiplatform security. *Energies, 12*(3), 402.

Koskinen, J., et al. (2008). How to use bibliometric methods in evaluation of scientific research? An example from finnish schizophrenia research. *Nordic Journal of Psychiatry, 62*(2), 136–143.

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41*(10), 1027–1038.

Kumar, S., & Kumar, S. (2008). Collaboration in research productivity in oil seed research institutes of India. In *Fourth international conference on webometrics, informetrics and scientometrics & ninth COLLNET meeting Humboldt- Universitat zu Berlin, Institute for Library and Information Science (IBI)* (pp. 1–18).

Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association, 24*(6), 1211–1220.

Lamiri, A., Gueraoui, K., & Zeggwagh, G. (2019). Bitcoin difficulty, a security feature. In *2nd international conference on Europe Middle East and North Africa information systems and technologies to support learning (EMENA-ISTL)*, (Vol. 111, pp. 367–372). Fez, Morocco.

Lee, D. H. (2019). Predictive power of conference-related factors on citation rates of conference papers. *Scientometrics, 118*(1), 281–304.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*, 1–13.

Li, J., & Shang, Y. (2019). Research on a suitable blockchain for IoT platform. In *Research on a suitable blockchain for IoT platform* (pp. 1063–1072).

Liu, Y., Lu, Q., Xu, X., Zhu, L., & Yao, H. (2018). Applying design patterns in smart contracts a case study on a blockchain-based traceability. *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)* (Vol. 10974, pp. 92–106).

Liu, J., Tian, J., Kong, X., Lee, I., & Xia, F. (2018b). Two decades of information systems: A bibliometric review. *Scientometrics, 118*(2), 617–643.

Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017). Blockchain based data integrity service framework for IoT data. In *24th IEEE international conference on web services, (ICWS)* (pp. 468–475). Honolulu, United States.

Liu, H., Zhang, Y., & Yang, T. (2018c). Blockchain-enabled security in electric vehicles cloud and edge computing. *IEEE Network, 32*(3), 78–83.

Lo, S. K., Xu, X., Chiam, Y. K., & Lu, Q. (2018). Evaluating suitability of applying blockchain. In *Proceedings of the IEEE international conference on engineering of complex computer systems, (ICECCS)* (pp. 158–161). Kyushu University, Fukuoka, Japan.

Loomes, D. E., & Van Zanten, S. V. (2013). Bibliometrics of the top 100 clinical articles in digestive disease. *Gastroenterology, 144*(4), 673–676.

Lopes, J., & Pereira, J. L. (2019). Blockchain technologies: Opportunities in Healthcare. In *International conference on digital science (DSIC)*, (Vol. 850, pp. 435–442). Budva, Montenegro.

Maesa, D. D. F., Marino, A., & Ricci, L. (2019). The graph structure of bitcoin. In *7th international conference on complex networks and their applications, (COMPLEX NETWORKS)* (pp. 547–558). Cambridge, United Kingdom.

Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications, 125,* 251–279.

Mao, G., Zou, H., Chen, G., Du, H., & Zuo, J. (2015). Past, current and future of biomass energy research: A bibliometric analysis. *Renewable and Sustainable Energy Reviews, 52,* 1823–1833.

Margheri, A. (2018). Differentially private data sharing in a cloud federation with blockchain. *IEEE Cloud Computing, 5*(December), 69–79.

Marsal-Llacuna, M. L. (2017). Future living framework: Is blockchain the next enabling network? *Technological Forecasting and Social Change, 128,* 226–234.

Memoria, F. (2019). No one knows what Venezuela's Petro Cryptocurrency is Actually Worth (Online). Available at https://www.ccn.com/no-one-knows-what-venezuelas-petro-cryptocurrency-is-actually-worth. Accessed February 18, 2019.

Mendling, J., et al. (2018). Blockchains for business process management—challenges and opportunities. *ACM Transaction on Management Information Systems, 9,* 1–16.

Miau, S., & Yang, J. M. (2018). Bibliometrics-based evaluation of the Blockchain research trend: 2008–March 2017. *Technology Analysis & Strategic Management, 30,* 1029–1045.

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017). A review on consensus algorithm of blockchain. In *IEEE international conference on systems, man, and cybernetics (SMC)* (pp. 2567–2572).

Mustaffa, Z., Sulaiman, M. H., & Kahar, M. N. M. (2015). LS-SVM hyper-parameters optimization based on GWO algorithm for time series forecasting. In *4th international conference on software engineering and computer systems, ICSECS 2015* (pp. 183–188). Virtuous Software Solutions for Big Data, Kuantan, Pahang.

Mustaffa, Z., & Yusof, Y. (2012). A hybridization of enhanced artificial bee colony-least squares support vector machines for price forecasting. *Journal of Computer Science, 8*(10), 1680–1690.

Oakleaf, M. (2009). Writing information literacy assessment plans: A guide to best practice. *Communications in Information Literacy, 3*(2), 80–90.

Parino, F., Beiró, M. G., & Gauvin, L. (2018). Analysis of the bitcoin blockchain: Socio-economic factors behind the adoption. *EPJ Data Science, 7*(1), 1–23.

Pass, R. N. (2019). Rafael N. Pass (Online). Available at https://www.engineering.cornell.edu/faculty-directory/rafael-n-pass. Accessed May 15, 2019.

Pass, R., & Shi, E. (2017). FruitChains: A fair blockchain Rafael. In *Proceedings of the ACM symposium on principles of distributed computing (PODC)* (pp. 315–324). DC, USA.

Pass, R., Shi, E. (2018). Thunderella: Blockchains with optimistic instant confirmation. *Lecture notes in computer science* (*including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics*) (Vol. 10821, pp. 3–33).

Puthal, D., & Mohanty, S. P. (2019). Proof of authentication: IoT-friendly blockchains. *IEEE Potentials, 38*(1), 26–29.

Rahouma, K. H. (2017). Reviewing and applying security services with non-english letter coding to secure software applications in light of software trade-offs. *International Journal of Software Engineering and Computer Systems (IJSECS), 3*(February), 71–87.

Razak, M. F. A., Anuar, N. B., Othman, F., Firdaus, A., Afifi, F., & Salleh, R. (2017). Bio-inspired for features optimization and malware detection. *Arabian Journal for Science and Engineering, 43*(12), 6963–6979.

Razak, M. F. A., Anuar, N. B., Salleh, R., & Firdaus, A. (2016). The rise of '"malware"': Bibliometric analysis of malware study. *Journal of Network and Computer Applications, 75,* 58–76.

Razak, M. F. A., Anuar, N. B., Salleh, R., Firdaus, A., Faiz, M., & Alamri, H. S. (2019). 'Less give more': Evaluate and zoning android applications. *Measurement: Journal of the International Measurement Confederation, 133,* 396–411.

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future Generation Computer Systems, 88,* 173–190.

Rimba, P., Binh, A., Ingo, T., Staples, M., Ponomarev, A., & Xu, X. (2018). Quantifying the cost of distrust : Comparing blockchain and cloud services for business process execution. *Information Systems Frontiers*, 1–19.

Rimba, P., Tran, A. B., Weber, I., Staples, M., Ponomarev, A., & Xu, X. (2017). Comparing blockchain and cloud services for business process execution. In *IEEE international conference on software architecture (ICSA)* (pp. 257–260). Sweden.

Roman, V., & Ordieres-Mere, J. (2019). IoT blockchain technologies for smart sensors based on raspberry pi. In *IEEE 11th international conference on service-oriented computing and applications IoT* (pp. 216–220). Paris, France.

Ryu, J. H., Sharma, P. K., Jo, J. H., & Park, J. H. (2019). A blockchain-based decentralized efficient investigation framework for IoT digital forensics. *The Journal of Supercomputing*, 1–16.

Smith, S. (2018). IoT connections to grow 140% to hit 50 billion by 2022, as edge computing accelerates RoI (Online). Available at https://www.juniperresearch.com/press/press-releases/iot-connections-to-grow-140-to-hit-50-billion. Accessed 6 Jan 2019.

Tahaei, H., Salleh, R., Razak, M. F. A., Ko, K., & Anuar, N. B. (2018). Cost effective network flow measurement for software defined networks: A distributed controller scenario. *IEEE Access, 6,* 5182–5198.

Tron Live, (2018). An easy to understand guide to PoW, PoS, DPoS, consensus mechanism and super representative (Online). Available at https://medium.com/tron-foundation/an-easy-to-understand-guide-to-pow-pos-dpos-consensus-mechanism-and-super-representative-eb1f5504a8e. Accessed 10 Dec 2018.

Vazirani, A., O'Donoghue, O., Brindley, D., & Meinert, E. (2018). Implementing blockchains for efficient healthcare: A systematic review. *Journal of Medical Internet Research, 21*(2), 1–12.

Wang, B., Chen, S., Yao, L., Liu, B., Xu, X., & Zhu, L. (2018). A simulation approach for studying behavior and quality of blockchain networks. *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)* (Vol. 10974, pp. 18–31).

Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., & Mendling, J. (2016). Untrusted business process monitoring and execution using blockchain. *Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics)* (Vol. 9850, pp. 329–347).

Wu, X., Chen, X., Zhan, F. B., & Hong, S. (2015). Global research trends in landslides during 1991–2014: A bibliometric analysis. *Landslides, 12*(6), 1215–1226.

Wu, D., Liu, X. D., Yan, X. B., Peng, R., & Li, G. (2019). Equilibrium analysis of bitcoin block withholding attack: A generalized model. *Reliability Engineering and System Safety, 185,* 318–328.

Xu, X., Pautasso, C., Gramoli, V., Ponomarev, A., & Chen, S. (2016). The blockchain as a software connector. In *13th working IEEE/IFIP conference on software architecture (WICSA)* (pp. 182–191). Venice, Italy.

Yuan, R., Bin Xia, Y., Chen, H. B., Zang, B. Y., & Xie, J. (2018a). ShadowEth: Private smart contract on public blockchain. *Journal of Computer Science and Technology, 33*(3), 542–556.

Yuan, B., Jin, H., Zou, D., Yang, L. T., & Yu, S. (2018b). A practical byzantine based approach for faulty switch tolerance in software-defined networks. *IEEE Transactions on Network and Service Management, 15*(2), 825–839.

Affiliations

Ahmad Firdaus[1] · Mohd Faizal Ab Razak[1] · Ali Feizollah[2] · Ibrahim Abaker Targio Hashem[3] · Mohamad Hazim[2] · Nor Badrul Anuar[2]

Ahmad Firdaus
firdausza@ump.edu.my

Ali Feizollah
ali.feizollah@siswa.um.edu.my

Ibrahim Abaker Targio Hashem
ibrahimabaker.targiohashem@taylors.edu.my

Mohamad Hazim
hazimhanif@um.edu.my

Nor Badrul Anuar
badrul@um.edu.my

[1] Faculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang, 26300 Gambang, Kuantan, Pahang, Malaysia

[2] Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia

[3] School of Computing, & IT, Taylor's University, 47500 Subang Jaya, Selangor, Malaysia