Journal of Industrial Information Integration 22 (2021) 100217

Contents lists available at ScienceDirect

Journal of Industrial Information Integration

journal homepage: www.sciencedirect.com/journal/journal-of-industrial-information-integration

Blockchain technology in the healthcare industry: Trends and opportunities

Hassan Mansur Hussien [a,*], Sharifah Md Yasin [a,b,*], Nur Izura Udzir [a], Mohd Izuan Hafez Ninggal [a], Sadeq Salman [c]

[a] Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia
[b] Institute for Mathematical Research (INSPEM), Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia
[c] Faculty of Engineering, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia

ARTICLE INFO

Keywords:
Bibliometric
Blockchain technology
Healthcare industries, information security
Privacy protection, Prospects

ABSTRACT

The growth in the use of blockchain technology in healthcare is remarkable and has a significant impact on the healthcare industry. In this work, the gap between the healthcare industry and blockchain technologies was addressed by evaluating previous activities. Bibliometric analysis of dataset distribution, venues, keywords and citations was conducted to identify the trend of blockchain technology in healthcare. Case studies of telecare medicine information system and E-health were also reviewed and evaluated in terms of security and privacy. This study discussed potential future challenges such as scalability and storage capacity, blockchain size, universal interoperability and standardisation. This work highlighted the motivations of employing blockchain technology in the healthcare industry. Prospects in health data and sharing process, clinical trials, the pharmaceutical industry, big data, artificial intelligence, 5 G ultrasonic device, security and privacy were highlighted.

1. Introduction

Blockchain technology has attracted numerous scholars, organisations and companies especially in the use of bitcoin, which is a digital cryptocurrency. A blockchain is a decentralised ledger that can securely store transactions made in a peer-to-peer network. Moreover, it makes transactions verifiable and transparent. The main aim of blockchain technology is to allow two parties to conduct transactions securely without any intermediary party intervention [1–8]. Numerous industries and sectors such as engineering, automotive, computing and electronic, aerospace, business and accounting, banking, defence and healthcare have been revolutionised by adopting smart technologies aside from blockchain, such as machine learning, Internet of Things (IoT), virtual reality and artificial intelligence (AI) [9–16].

The use of blockchain technology in the healthcare industry has enhanced the transparency and communications between patients and healthcare providers [17]. The size and complexity of healthcare records are growing but have not yet been optimised because of duplicates, the use of different names and identifiers, and their availability in different networks [18]. Furthermore, healthcare security has become important to keep data secure and prevent criminal activities. If unlicensed users are allowed to access patient data, then the data can be used or sold, with personal information of patients being shown to anyone with access. The privacy of patients' data is vital to efficacious healthcare management [19]. These issues and concerns can be solved by employing blockchain technology supported by Industry 4.0 to ensure the integrity of data and prevent tampering and failure at any single point [20–22].

Many scholars have reviewed the impact of blockchain technology in the healthcare industry [23–31]. The main focus of their reviews and surveys is the significant enhancement in security, privacy, data sharing and ability to transfer data between two parties without obstacles and

Abbreviation: 5 G, **Fifth-generation mobile network technology**; **AI**, Artificial intelligence; **AES**, Advanced Encryption Standard; **CP-ABE**, ciphertext-policy attribute-based encryption; **EEG**, Electroencephalography; **EHRs**, Electronic health records'; **EMR**, Electronic Medical records'; **FHIR**, Fast Healthcare Interoperability Resources; **HL7**, Health Level Seven International; **IHE**, Integrating the Healthcare Enterprise; **IoMT**, Internet of Medical Things; **IoT**, Internet of Things; **IPFS**, InterPlanetary File System; **PBFT**, Practical Byzantine fault tolerance; **PEKS**, Public key encryption with keyword search; **PHRs**, Personal health records; PoA, Proof of authority; **PoS**, Proof of stake; **PoW**, Proof of work; **PSN**, Pervasive social network; **RESTful API**, Representational state transfer; **RPM**, Remote patient monitoring; **RSA**, Rivest–Shamir–Adleman public-key cryptosystem; **TMIS**, Telecare medical information systems.

* Corresponding authors.
E-mail addresses: hassanalobady@gmail.com (H.M. Hussien), ifah@upm.edu.my (S.M. Yasin), izura@upm.edu.my (N.I. Udzir), mohdizuan@upm.edu.my (M.I.H. Ninggal).

https://doi.org/10.1016/j.jii.2021.100217
Received 13 April 2020; Received in revised form 8 November 2020; Accepted 2 March 2021
Available online 4 March 2021

preventing unauthorised users by employing blockchain technology. Some healthcare applications require specific criteria that may not be addressed by the adoption of blockchain, such as authentication, interoperability and sharing of records due to demanding legal requirements.

There is a lack of bibliometric studies of blockchain technology in the industry of healthcare. To fill the void, this study covers blockchain technology and healthcare studies. Also, the study addresses future research paths in appropriate scope and breadth in relevant fields. A road map of state-of-the-art review of blockchain technology that can be applied in healthcare is given in **Fig. 1**. As shown in the figure, this study aims to summarise the results of the bibliometric analysis with the distribution of data, keywords, venues, and distribution of citations. This review also presents telecare medical information systems (TMIS) and E-health system studies and their evaluations of privacy and security. Additionally, this study provides insight into the role and features of blockchain technology in the healthcare sector by highlighting motivations and challenges. Blockchain and healthcare prospects in the parameters of security and privacy, clinical trials, and healthcare sharing processes are pointed out. Overall, this work presents a review of blockchain technology in healthcare industries.

The subsequent sections are as follows: The research methodology is presented in **Section 2**. The background of blockchain technology and its fundamentals are summarised in **Section 3**. The bibliometric analysis and its discussion are presented in **Section 4**. Case studies of blockchain technology and healthcare industry are explained in **Section 5**. The discussion, which includes challenges and motivations, is organised in **Section 6**. Finally, the prospects for scholars and organisations are given in Section 7.

2. Research methodology

This study concentrates on blockchain technology in the healthcare industry. This section explains the method used in this research. **Fig. 2** shows the phases of this study: extraction, preprocessing, analysis and visualisation of the dataset. The dataset contains details on the healthcare industry and blockchain technology as indexed by Web of Science (WoS) and Scopus from 2016 to 2020. In this research, bibliometric analysis of blockchain technology in the healthcare industry is conducted by using the open-source statistical system R. The package of [32] is installed and used in the R desktop system. Numerous studies

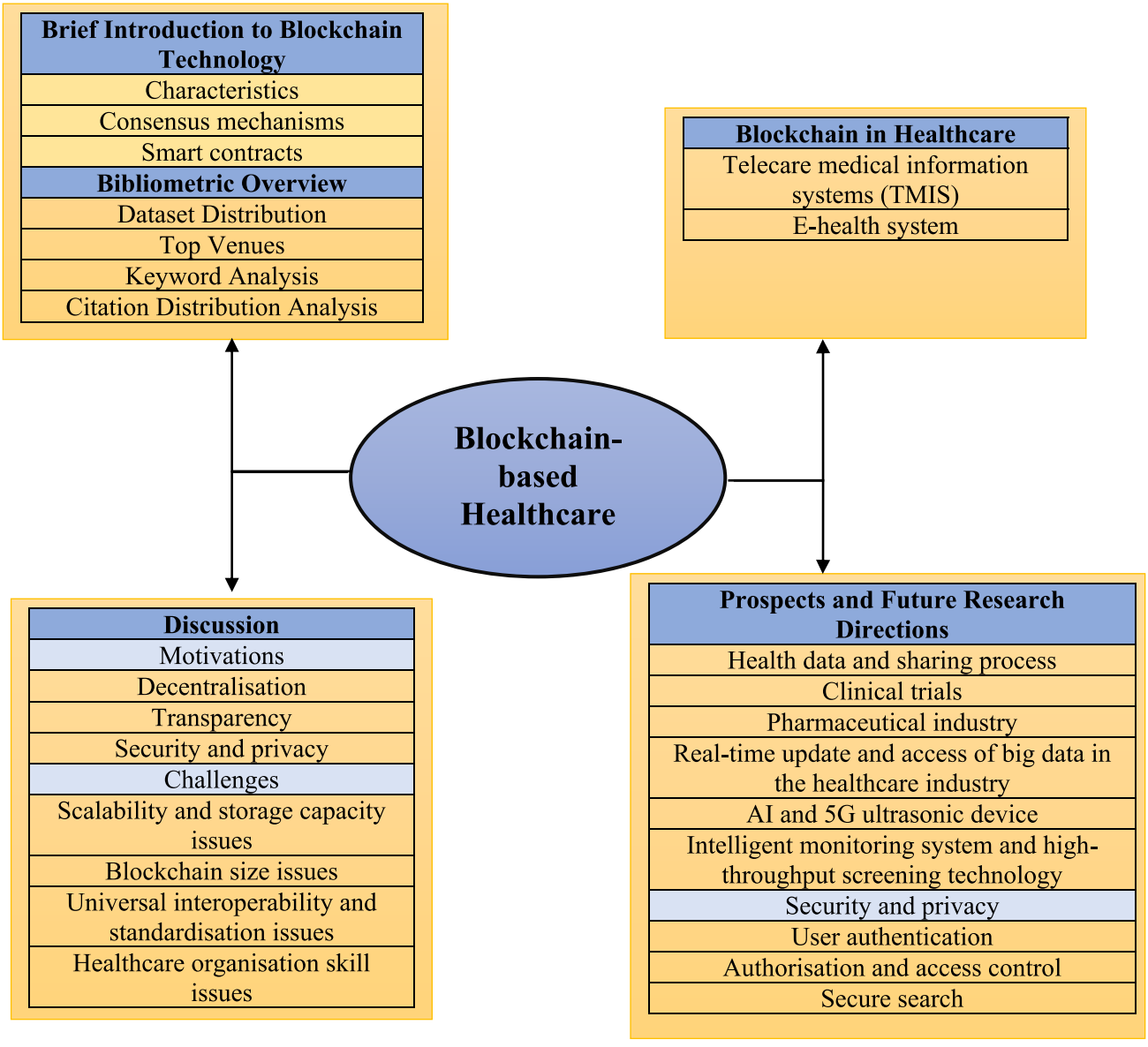

Fig. 1. Road map of blockchain-based healthcare industry.

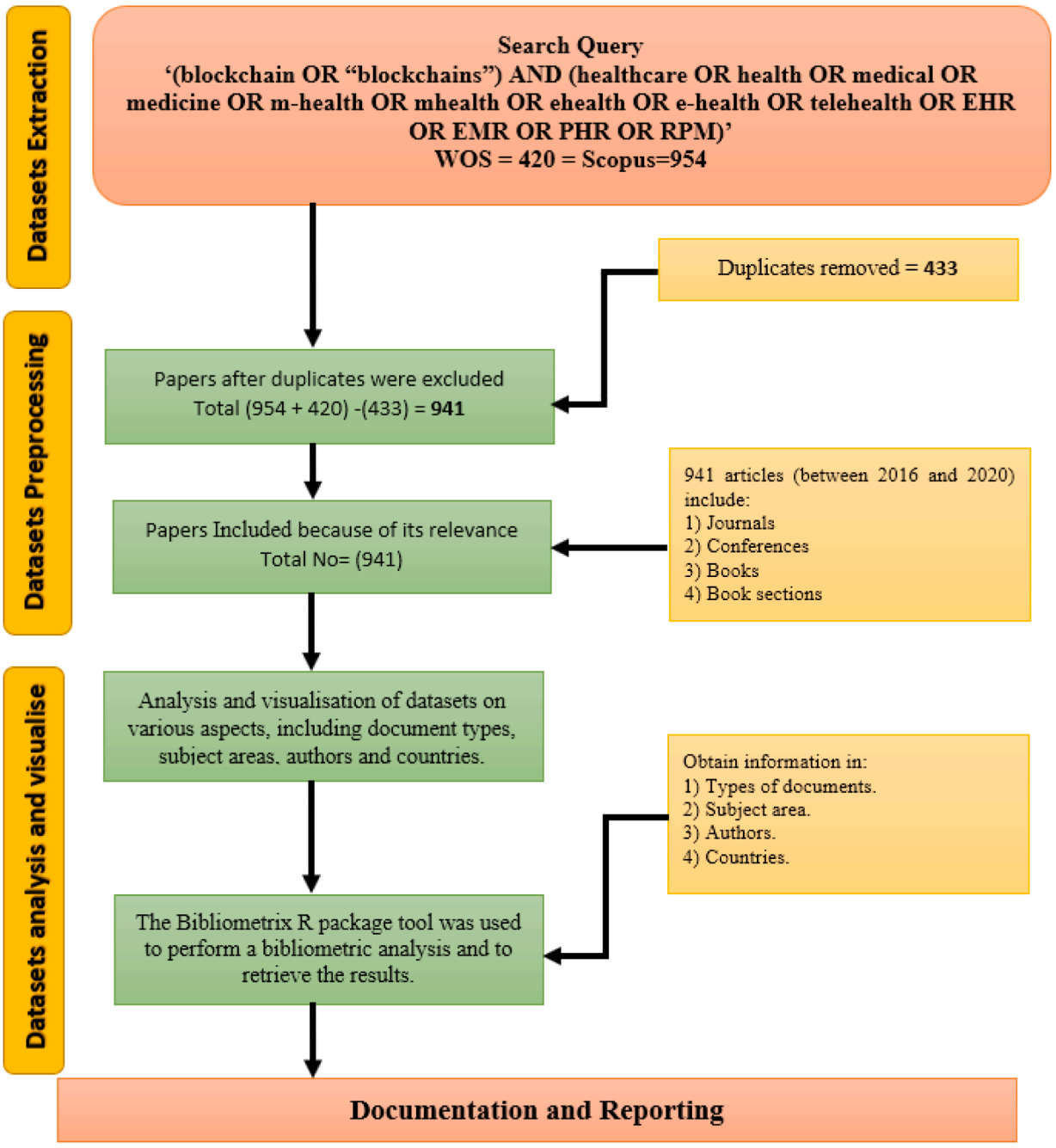

Fig. 2. Research methodology flow.

have used this bibliometrics tool for their specific research fields [33–39].

3. Brief introduction to blockchain technology

Blockchain technology has a novel, integrated, unique and innovative computing technology that includes decentralised peer-to-peer networking, decentralised storage, transparent transactions, intelligent consensus mechanisms, dynamic public key encryption algorithms and a programmable smart contracts [40]. This technical aspect of the blockchain system architecture constructs a sustainable, secure and efficient network system whose applications are precisely needed to address issues [9–11]. An overview of the architecture of the blockchain contents of the three layers is illustrated in Fig. 3. The network layer defines a peer-to-peer connection to secure tasks or workloads between node peers in a decentralised environment. The blockchain transaction layer maintains the immutable data of entities with cryptographic protocols. The transaction's structure formulates the data entities of the node into the chain of blocks by using a Merkle tree. The application layer allows the developer to implement a decentralised application on the available blockchain platform, such as Ethereum and Hyperledger, with the aid of a smart contracts.

3.1. Characteristics of blockchain innovation

The main aspect of the blockchain is decentralisation, where all information is stored permanently and securely without requiring a centralised authority to control the transactions. With regard to this significant enhancement, the entities engaged with the blockchain are required to agree on events in a peer-to-peer network manner by using a

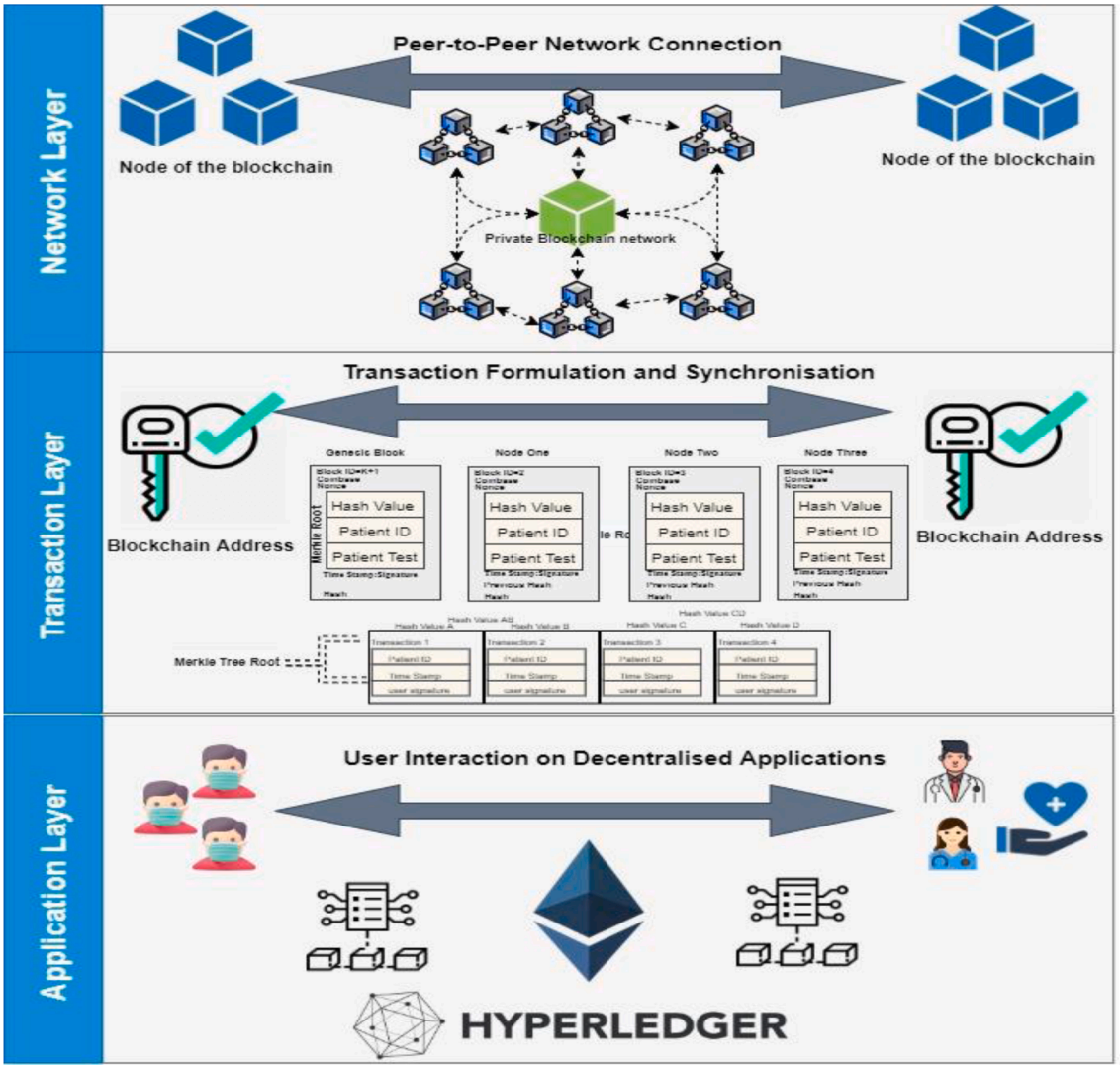

Fig. 3. Blockchain architecture.

variety of consensus protocols. The other aspect of the blockchain characteristic is the tamper-proof quality of the stored information. The fundamental idea beyond being tamper-proof is that the details must be essentially impossible to alter or entities cannot be changed upon being approved on the blockchain because its distributed ledger is stored across multiple nodes [41,42]. The blockchain maintains the privacy of transactions provided by the pseudonymity feature, as extensively investigated and implemented in different applications and sectors [7, 12,40,43,44].

Lately, blockchain technology has been attracting scholars and companies due to the characteristics of the audit and traceability possibilities by integrating a released new block into another previous block by using the hash function to construct a chain of blocks. The data structure of the Merkle tree is used to format the transaction data on the blockchain network, where each transaction leaf can be inspected by the defined root [45]. Concepts beyond the tree structure enable the integrity and immutability of the data stored on the blockchain [14]. Fig. 4 illustrates the visual representation of the basic data structure of the blockchain.

3.2. Consensus mechanisms

The most attractive feature integrated into blockchains is how the entities are authorised and how transaction data are validated by using the distributed consensus protocol. These transactions can be approved in the distributed ledger transaction pool, which contains all unverified transactions for the upload and access of data stored in the blockchain. Each blockchain event is categorised into data blocks and transmitted to the transaction pool to be verified by the miners to be appended on the main network of the blockchain. To validate and synchronise the block with its signature in chronological order, the miners perform a consensus mechanism and each entity node receives a copy of the block to be verified. Several consensus mechanism algorithms have been proposed in the literature, but the most commonly used types of algorithms are the following [46,47]:

Proof of work (PoW): This consensus mechanism is a secure algorithm used in the blockchain and was first integrated into the bitcoin cryptocurrency application. The core idea of the PoW protocol is that miners need to solve a computationally difficult puzzle game by finding the hash of the block submitted to the transaction pool with a value lower than the default. The miner who can solve this puzzle game is allowed to append the block in the network and receive a certain amount of bitcoin reward [48]. The current PoW protocol has major drawback; it consumes a large amount of energy and computational power, and it is unsuitable for large-scale healthcare applications [49].

Proof of stake (PoS): This consensus protocol depends on the assets of the entities. The entities can only validate and confirm a new block if the proportion of assets, i.e. wealth or stake, is higher in the blockchain

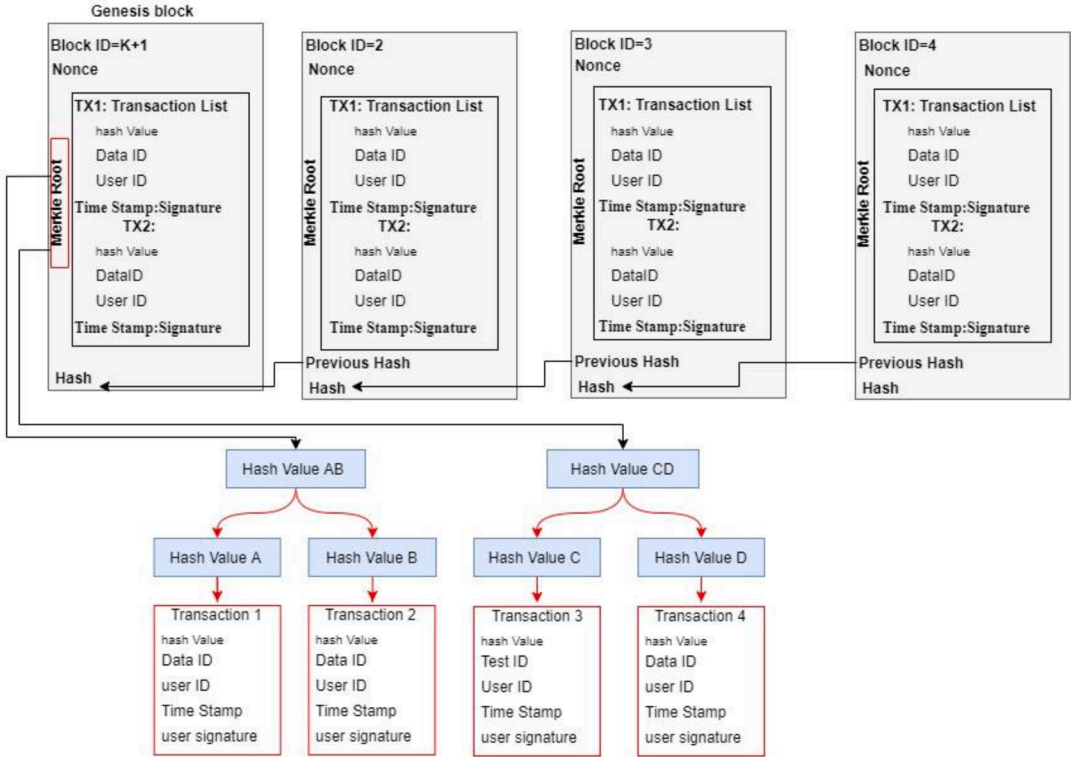

Fig. 4. Data block structure.

network. From the practical perspective of cryptocurrency, entities are required to predetermine a minimum amount of their asset value deposit. Moreover, the PoS eliminates the competition game of solving a computationally difficult puzzle, thereby decreasing computational power consumption compared with the PoW [50]. However, the ideology of the PoS consensus protocol is still undesirable in some healthcare organisations and developers because it is more suitable in the era of cryptocurrency applications.

Practical Byzantine fault tolerance (PBFT): This consensus protocol is reliant on Byzantine agreement technology [51]. The core idea of the PBFT is that all the entities need to be predefined in the blockchain network. The PBFT consensus mechanism process consists of five phases: request, pre-prepare, prepare, commit and reply events. The entity in the blockchain network needs a maximum of two replica votes from all the connected nodes to be processed throughout the phases. The adoption of the PBFT consensus algorithm in blockchain technology can significantly reduce energy consumption and is considered more appropriate for the current structure of healthcare applications [52].

3.3. Smart contracts

Recent interest in blockchain technology has given new impetus to the use of a smart contracts to implement it in the main network. The advent of smart contracts provides vast benefits toward blockchain by eliminating intermediaries and supporting features such as self- and auto-executing, immutability and self-verification. The Ethereum blockchain infrastructures introduce the idea of smart contracts by providing the opportunity for the developer to implement a number of decentralised applications in the financial and non-financial sectors [41, 45,48]. Solidity is the most mature and complete high-level smart contracts programming language that enables decentralised applications to be implemented in the way predefined contracts are run on the main blockchain network. This functionality within the platform of the smart contracts breakthrough in the blockchain is expected to offer promising solutions for the healthcare sector [53].

4. Bibliometric overview

This section presents a bibliometric analysis of the use of blockchain in the healthcare industry on the basis of the following aspects: (1) dataset distribution, (2) top venues, (3) keyword analysis and (4) citation distribution analysis. These findings will help healthcare professionals and policymakers promote blockchain adoption in the healthcare sector.

4.1. Dataset distribution

This section reveals the main information of the data extracted from WoS and Scopus databases. A total of 941 articles were published between 2016 and 2020, as shown in Table 1. These articles were published in various research format sources, such as journals, books, conferences and proceedings. The keyword, authors, citations and annual articles are tabulated in Table 1. Fig. 5 illustrates the extracted

Table 1
Main information.

Sources	No.
Articles	941
Sources (journals, books, etc.)	434
Keywords plus (ID)	3594
Author's keywords (DE)	1640
Author appearances	3099
Authors of single-author articles	62
Authors of multi-author articles	2316
Authors per article	2.53
Co-authors per articles	3.29
Average citations per article	5.798
Collaboration index	3.17
2016	15
2017	76
2018	261
2019	511
2020	78

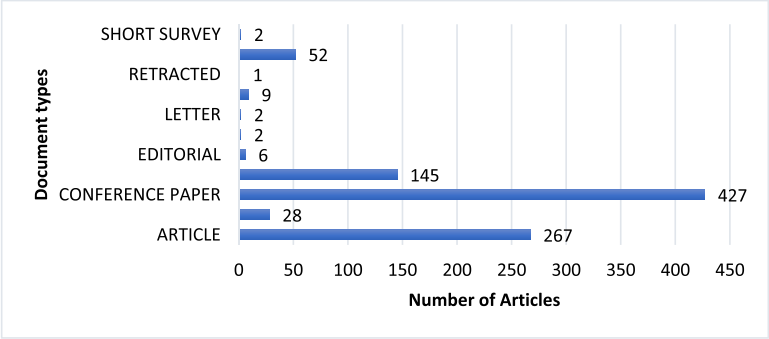

Fig. 5. Source classification.

data and the number of articles in each source.

Fig. 6 shows the annual production of the articles. The publication rate shows annual increases with an annual growth rate of 51.01%. Recently, blockchain and the healthcare system have attracted increasing interest from academia and industry. The growth of blockchain developments in the healthcare system increased dramatically in 2019, and further research is expected to be conducted in 2020. This finding indicates that the use of blockchain in the industry is an evolving area and provides a great opportunity for scholars and organisations. Fig. 7 illustrates that the number of blockchain publications in academic aspects has increased each year, which shows the significance of blockchain in the field of healthcare research.

Fig. 7 shows the proportions of blockchain studies in the healthcare industry. The figure indicates the increasing trend of healthcare studies and blockchain technology. The subject is expected to be investigated widely in 2020 because of its importance in monitoring patients remotely during pandemic situations such as COVID-19, Ebola, SARS, and MERS. Table 2 shows the time trend of blockchain studies in the healthcare industries. Findings indicate that publications on blockchain-based healthcare systems are increasing dramatically.

4.2. Top venues

This section presents the academic papers categorised according to the journals and scientific conferences of publishers. This categorisation was used in the literature bibliometric analysis to assist scholars in targeting the appropriate journal related to the subject of the study. Table 3 presents the top 20 publication venues for academic papers in accordance with the blockchain and healthcare industry publication domains in ascending order.

Series and publications such as *Lecture Notes in Computer Science* and *Advances in Intelligent Systems and Computing* published the highest number of articles and are considered popular publisher venues. The most popular journals that have published research articles are *IEEE Access, Journal of Medical Internet Research, Journal of Medical Systems, Sensors, Electronics* and *Future Generation Computer Systems*. Fig. 8 explains the dynamic growth of publishers in the temporal pattern, revealing that *IEEE Access* will expect an increase in the number of blockchain publications in the future. These publishers have the largest number of citations, indicating that the blockchain and healthcare system domains are closely linked to research articles.

Fig. 9 shows the top-ranked areas in the development of healthcare industry and blockchain technology. On the basis of the percentage with respect to healthcare and blockchain publications, computer science ranks first (38%) follows by engineering (20%) and medicine (9%). The other research areas are mathematics (8%), decision sciences (7%), social sciences (5%), business, management and accounting (4%), physics and astronomy (3%), materials science (1%), health professions (1%) and multidisciplinary (1%. Each research paper covers more than one area in the form of multidisciplinary research. This trendy research area is presented to provide scholars with great opportunities to discover new lines of research.

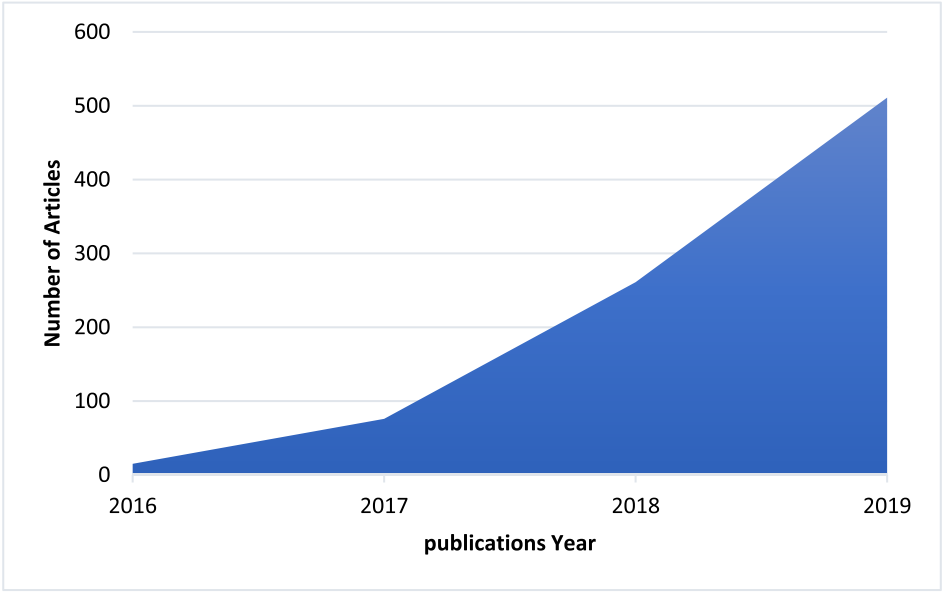

Fig. 6. Annual scientific production.

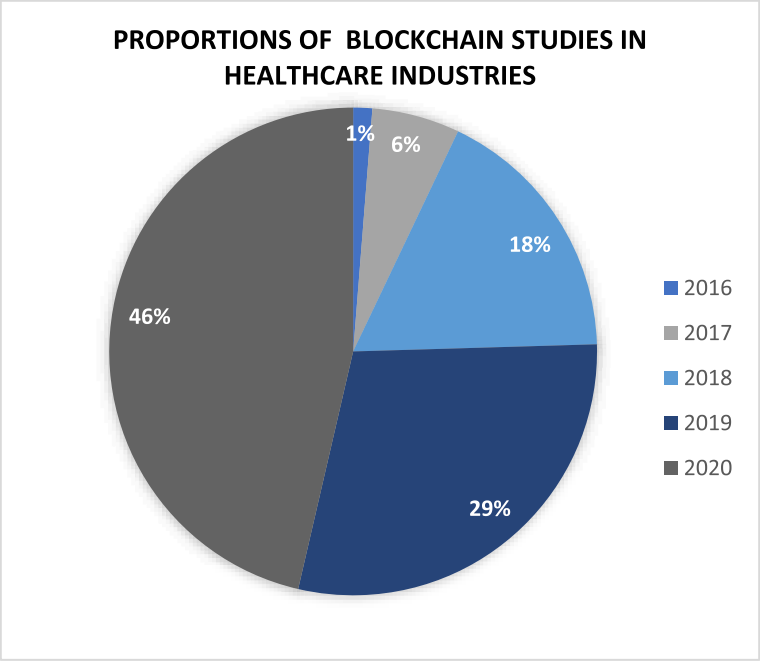

Fig. 7. Yearly publication trend.

Table 2
Time trend of blockchain-based healthcare system studies.

Years	Healthcare industries studies	Blockchain and healthcare industries	Blockchain studies in healthcare industries percentage
2016	19,500	15	0.077%
2017	21,132	76	0.36%
2018	24,300	261	1.074%
2019	28,530	511	1.791%
2020	2722	78	2.866%

Table 3
Top 20 publishing venues that involved blockchain.

Venue Name	Number of Articles
Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	62
Advances in Intelligent Systems and Computing	34
IEEE Access	32
ACM International Conference Proceeding Series	31
Communications in Computer and Information Science	30
Journal of Medical Internet Research	19
Journal of Medical Systems	18
Proceedings – IEEE 2018 International Congress on Cybermatics: 2018 Ieee Conferences on Internet of Things Green Computing and Communications Cyber Physical and Social Computing Smart Data Blockchain Computer and Information Technology Ithings/Greencom/Cpscom/Smartdata/Blockchain/Cit 2018	18
Studies in Health Technology and Informatics	15
Ceur Workshop Proceedings	12
Lecture Notes in Business Information Processing	11
Lecture Notes of The Institute for Computer Sciences Social-Informatics and Telecommunications Engineering	11
Advanced Sciences and Technologies for Security Systems	9
Sensors (Switzerland)	9
Electronics (Switzerland)	8
International Journal of Recent Technology and Engineering	8
Procedia Computer Science	8
Smart Innovation Systems and Technologies	8
Future Generation Computer Systems	7
Lecture Notes in Electrical Engineering	7

4.3. Keyword analysis

This section analyses keywords to identify research gaps in the integration of blockchain technology within the healthcare system. The most frequently used keywords in research on blockchain technology in the healthcare industry are presented in descending order. Table 4 shows the top 20 most frequent keywords; the keywords 'blockchain', 'smart contracts', 'healthcare', 'security' and 'privacy' appeared 574, 127, 87, 76 and 65 times, respectively. This result reveals that most studies on blockchain-based healthcare industry focus on the development of a decentralised network to solve a single security failure problem.

This decentralised technique notably minimises the system configuration cost, maintenance, arbitration and adjustment in the communication case, where it is implemented once in a centralised place. Regardless of the high performance in several conditions, this system encourages the solving of a single point of failure. The term that described procedures and rules is smart contracts, which appeared 127 times, as shown in Table 4. This term clearly has a significant impact on the blockchain and healthcare industry. Using a smart contracts allows researchers and organisations to access personal health data and to benefit patients [54–56].

Given the challenges posed by the Internet of Things (IoT), such as security and privacy, blockchain has contributed to the Internet of Medical Things (IoMT) to solve the mentioned challenges. IoT appeared 59 times, as shown in Table 4. 'Ethereum' appeared 33 times. 'Electronic health records' (EHRs) and 'personal health records' (PHRs) appeared 56 times along with other words such as 'interoperability and authentication', 'machine learning', 'access control' 'data sharing', 'decentralisation' and 'cloud computing', which appeared 27, 20, 20, 19, 19 and 18 times, respectively. This finding indicates that research is being conducted on the use of blockchain technologies to improve the security of shared medical data in terms of user authentication and access control. Other interesting keywords were identified, such as telemedicine (16), diagnosis (13), health care providers (10) and health information exchange (7). This research field is just beginning to use the advantage of blockchain technology to address some problems in the conventional remote medical diagnosis framework.

Fig. 10 shows the research papers involved in the blockchain and

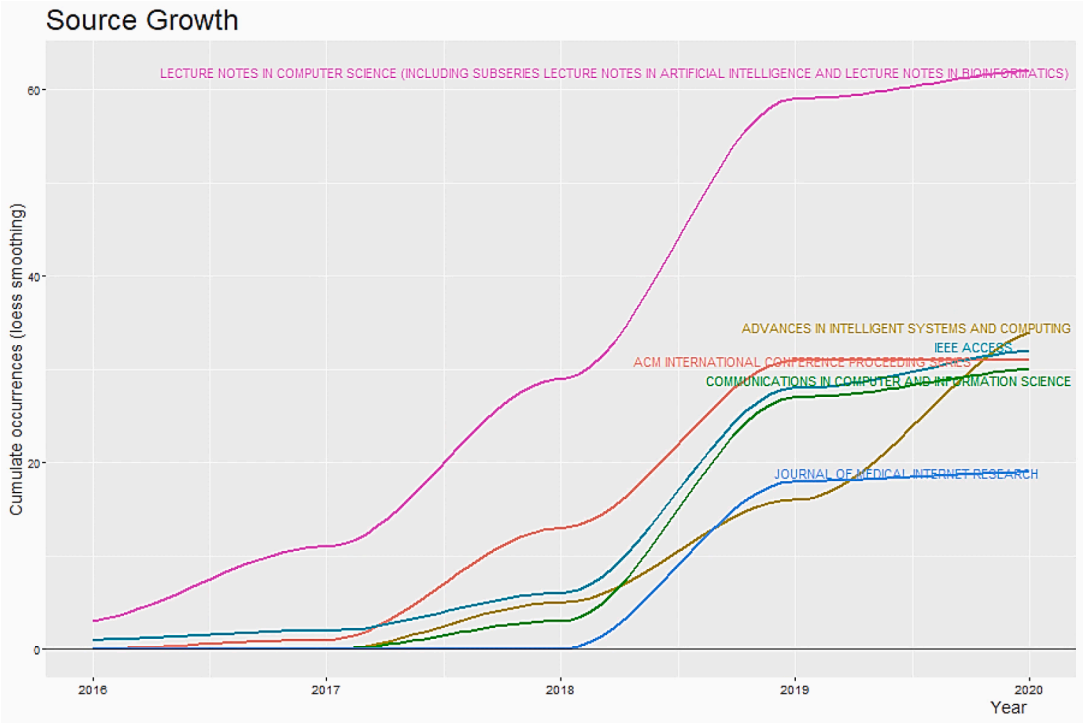

Fig. 8. Source growth.

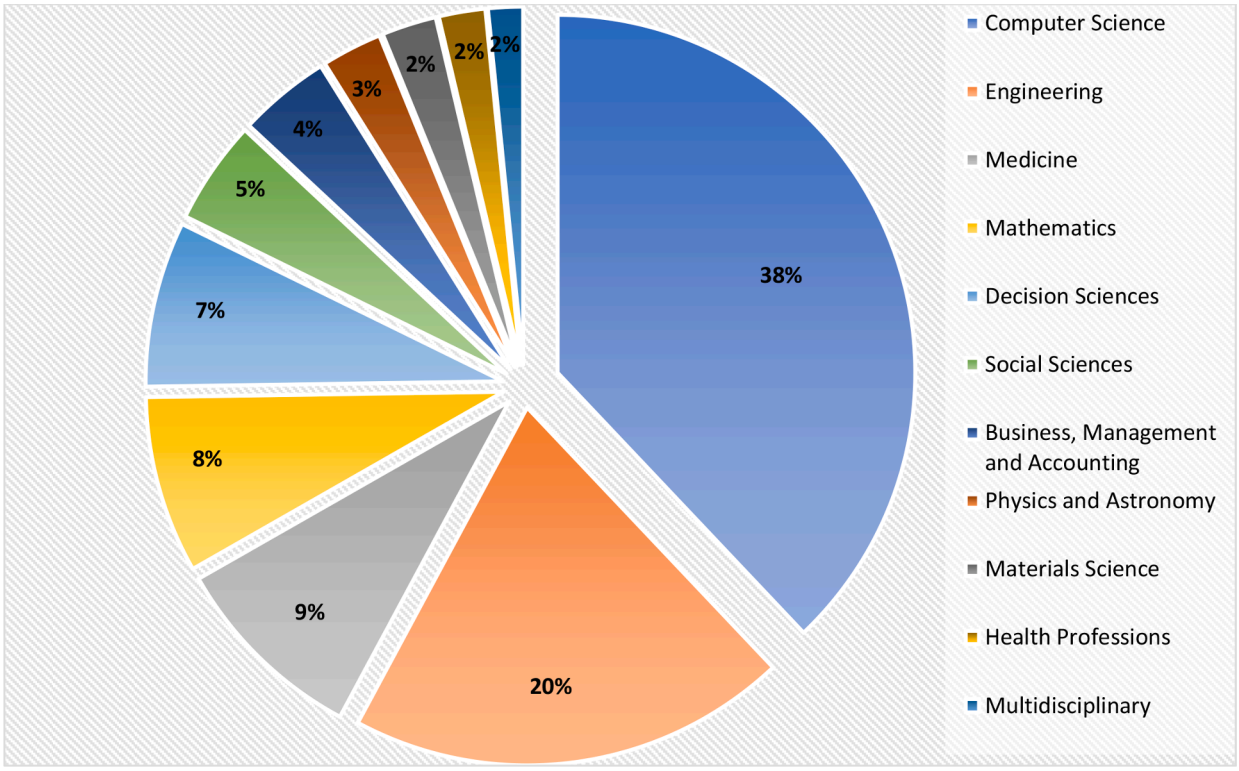

Fig. 9. Top 10 relevant research areas.

healthcare industry as a word cloud. The word cloud indicates that blockchain in the healthcare system has a high potential in these areas of study and would represent an increase in the number of publications in the future. To summarise the keywords that the word cloud provides and define the most significant keywords that attract research, three security areas are highlighted: (1) authentication, (2) access control and (3) data privacy. This finding indicates that security professionals are interested in applying blockchain to strengthen security and privacy. This result confirms that scholars believe in blockchain technology and include it in their work to secure data of IoT devices, protect people's identity and prevent data from being attacked.

Fig. 11 shows a co-occurrence network topological structure of high-

Table 4
Most frequent keywords.

No	Keywords	Occurrences
1	Blockchain	574
2	Smart contracts	127
3	Healthcare	87
4	Security	76
5	Privacy	65
6	Internet of Things	59
7	Ethereum	33
8	Electronic health records	30
9	Interoperability	27
10	Personal health records	26
11	Authentication	20
12	Machine learning	20
13	Access control	19
14	Data sharing	19
15	Decentralisation	19
16	Cloud computing	18
17	Telemedicine	16
18	Diagnosis	13
19	Healthcare providers	10
20	Health information exchange	7

frequency words in blockchain studies on healthcare. The high-frequency words in the blockchain and healthcare are demonstrated by a node. The relation between two high-frequency words in all blockchain studies on healthcare is represented by an edge. The degree of the node is the key measure that indicates the significance of the node in the network. Often, a large degree of nodes is considered when the nodes or the hub nodes have a high connectedness. The co-occurrence network recorded further that high-frequency words in blockchain and healthcare literature include 'blockchain', 'smart contracts', 'IoT', 'EHRs', 'cloud computing', 'AI' and 'supply chain'. This evidence indicates that blockchain is considered effective by security professionals in ensuring security and helping recover and save human lives.

4.4. Citation distribution analysis

This section analyses papers' citations in the blockchain-based healthcare system. Fig. 12 shows the top countries that are leading in the domain of blockchain and healthcare. The listed countries attempted to employ blockchain technology in the healthcare industry, such as PHRs and EHRs. Another interesting aspect is the integration of blockchain with TMIS in various case studies, such as remote patient monitoring (RPM) system, teledermatology, teleradiology, telerehabilitation and telesurgery.

The most cited countries were discussed. Studying the country citations can indicate the significance of each country in blockchain and healthcare studies. The USA is the most productive and influential country in the area of blockchain-based healthcare system with more than 560 citations. Finland ranks second with more than 354 citations, followed by China with 305 citations. Switzerland, Italy and France have 154, 142, and 115 citations, respectively. Greece, Taiwan, Korea, Hong Kong, Australia, India, Brazil, Macedonia, Singapore, Japan, Canada, the United Kingdom, Spain and Thailand all have fewer than 100 citations.

Table 5 lists the top 10 cited articles. The work of Yue et al. [57] has the largest number of citations. An HDG-centric healthcare ecosystem was built on the basis of a blockchain to make it easy to secure and easily accessible to the patient while preserving private patient information. The second most cited paper is presented in [58], which was published in 2017 and has 234 citations. It proposed MeDShare to address the issue of medical data sharing amongst big data custodians in a trustless environment. MeDShare monitors data sharing cloud repositories between large data entities, and the recorded medical data are stored in a tamper-proof manner by using blockchain.

The third most cited article is [59], which was published in 2016 with 127 citations. It proposed pervasive social network (PSN)-based healthcare on the basis of two protocols. The first procedure was improved on the IEEE 802.15.6, which shows an authenticated suggestion by launching secure connections with unbalanced computational necessities for mobile devices and resource-limited sensor nodes. The second procedure uses blockchain technology to share health data between PSN nodes. The fourth most cited article is [60], which was published in 2018 and proposed an innovative user-centric health data sharing solution through the use of blockchain's decentralised and permissioned membership service features to protect privacy and enhance identity management. The fifth most cited article was published

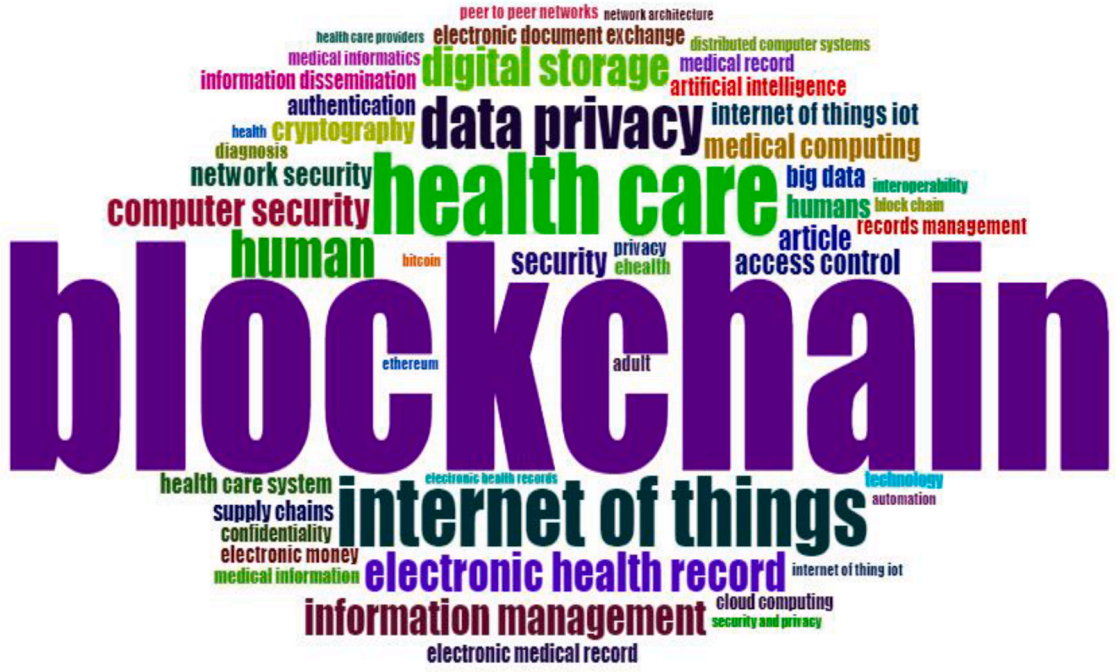

Fig. 10. Word cloud of blockchain in healthcare system keywords.

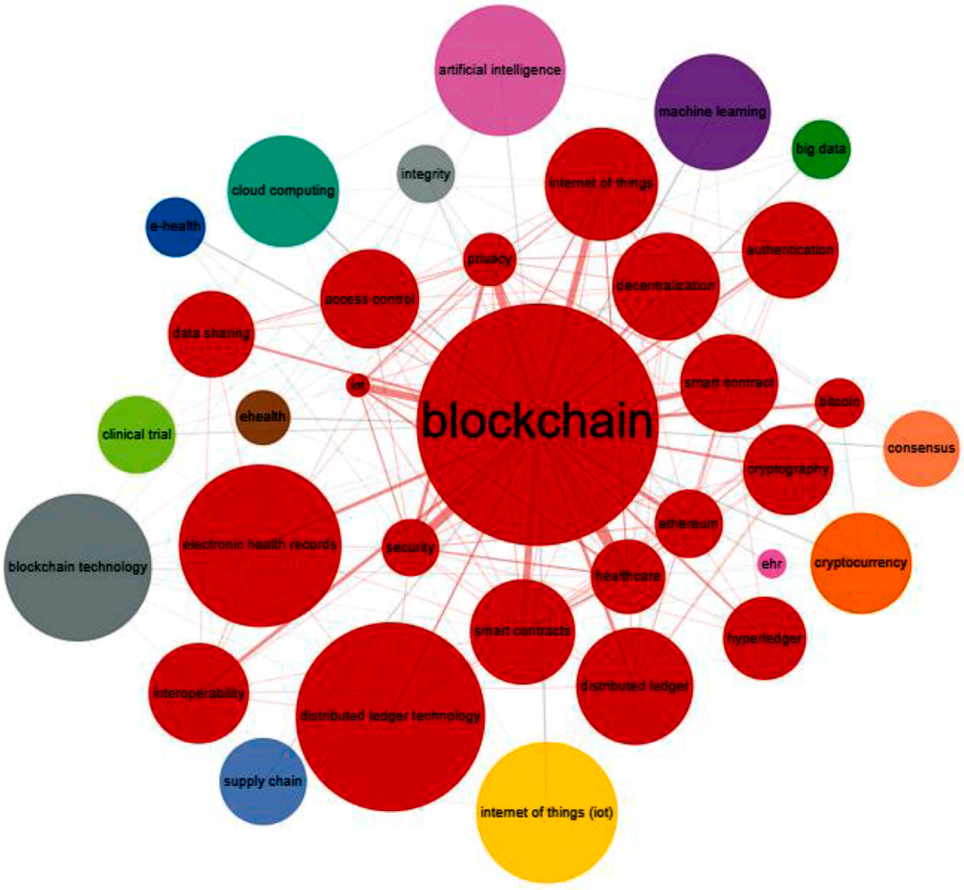

Fig. 11. Keyword co-occurrence network.

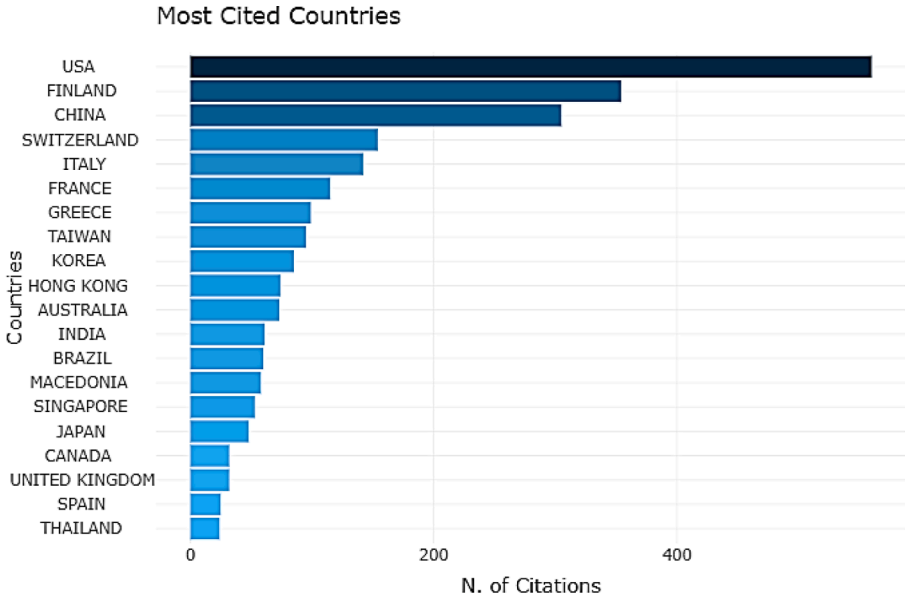

Fig. 12. Top countries.

in 2018 [61]; it developed an encapsulated EHR using blockchain features to ensure the validity of medical data, as well as an access control based on multiple authorities' attribute-based signature scheme to protect the privacy of patient data.

The sixth most cited article was published in 2018 [55], and it proposed a system based on blockchain and smart contracts to simplify medical sensor analysis and management security in the remote patient monitoring field. The seventh most cited article was published in 2017 [62], and it developed a blockchain-based PHR system to offer a distributed and interoperable PHR architecture model that provides a unified perspective for patients and healthcare providers. The eighth most cited article was published in 2019 [63], and it proposed a novel

Table 5
Details of the most 10 cited papers.

Title	Authors	Publisher	Rank	Year	Citation	Corresponding Author's Country
Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control [57]	Xiao Yue, Huiju Wang, Dawei Jin, Mingqiang Li and Wei Jiang	*Journal of Medical Systems*	IP=2.415/ Q2	2016	397	China
MeDShare: Trust-Less Medical Data Sharing amongst Cloud Service Providers via Blockchain [58]	Qi Xia, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, And Mohsen Guizani	*IEEE Access*	IP=4.098/ Q1	2017	234	China
A Secure System For Pervasive Social Network-Based Healthcare [59]	Jie Zhang, Nian Xue And Xin Huang	*IEEE Access*	IP=4.098/ Q1	2016	127	China
Integrating blockchain for data sharing and collaboration in mobile healthcare systems[60]	Xueping Liang, Juan Zhao, Sachin Shetty, Jihong Liu Danyi Li	*IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*	non	2018	127	China
Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in EHR Systems[61]	Rui Guo, Huixian Shi, Qinglan Zhao And Dong Zheng	*IEEE Access*	IP=4.098/ Q1	2018	117	China
Healthcare blockchain system using smart contracts for secure automated remote patient monitoring[55]	Kristen N. Griggs, Olya Ossipova, Christopher P. Kohlios, Alessandro N. Baccarini, Emily A. Howson, Thaier Hayajneh	*Journal of Medical Systems*	IP=2.415/ Q2	2018	98	USA
OmniPHR: A distributed architecture model to integrate personal health records[62]	Alex Roehrs, Cristiano André da Costa and Rodrigo da Rosa Righi	*Journal of Biomedical Informatics*	IP=2.950/ Q1	2017	86	Brazil
A decentralised privacy-preserving healthcare blockchain for IoT[63]	Ashutosh Dhar Dwivedi, Gautam Srivastava, Shalini Dhar and Rajani Singh	*Sensors Mdpi*	IP=3.031/ Q1	2019	73	Canada
MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain[64]	Kai Fan, Shangyang Wang, Yanhui Ren, Hui Li and Yintang Yang	*Journal of Medical Systems*	IP=2.415/ Q2	2018	58	China
Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain [65]	Aiqing Zhang and Xiaodong Lin	*Journal of Medical Systems*	IP=2.415/ Q2	2018	57	China

framework of modified blockchain models suitable for IoT devices that depend on their distributed nature and other additional privacy and security characteristics in the remote patient monitoring network.

The ninth most cited work was published in 2018 [64], and it proposed MedBlock, which is a blockchain-based patient information management system for handling patient information stored in the

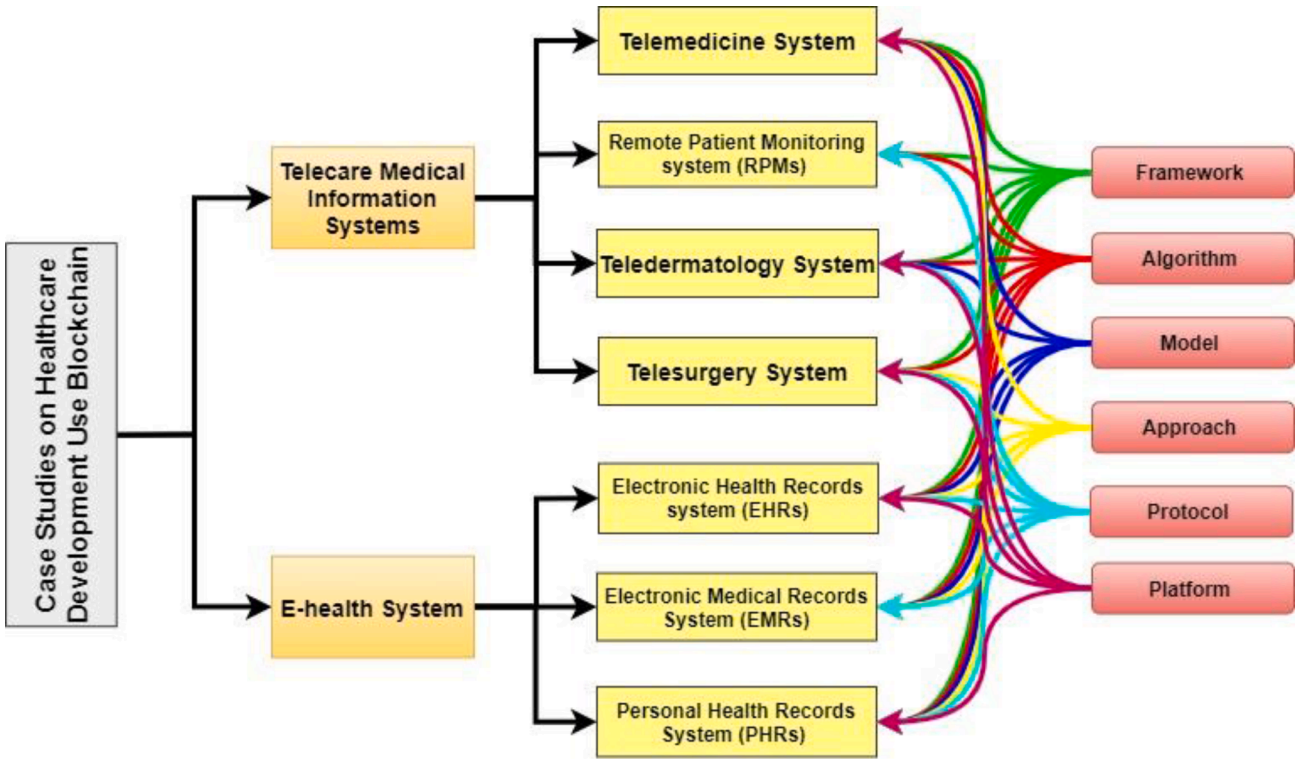

Fig. 13. Healthcare system development using blockchain taxonomy.

distributed ledger and improved access and retrieval of EMRs.

The tenth most cited work was published in 2018 [65], and it proposed a secure personal health information system based on blockchain technology to boost patient diagnosis in E-health systems.

5. Blockchain in healthcare

Blockchain technologies have the potential to shift the topology of a healthcare network into decentralised manner in which data are appended. Blockchain enables patients to place themselves in an ecosystem environment while enhancing the security, confidentiality and interoperability of data. This section explains the healthcare development system, which includes the approach, architecture, algorithm, scheme, framework, platform, model or protocol on the basis of the blockchain. Fig. 13 illustrates the taxonomy of the present healthcare system development in blockchain technology.

5.1. Telecare medical information systems (TMIS)

The integration of the blockchain technology into the application of TIMS content of three layers as shown in Fig. 14. The wireless body sensor layer is a content group of patients who are connected to the sensors to monitor their health conditions for diagnostic purposes, such as surgery, hospital visits and monitoring of elderly patients at home. The blockchain network is responsible for storing, sharing, updating the healthcare player's entities. Healthcare providers are a group of health professionals, such as physicians, hospitals, health insurance, medical organizations, who seek better and more accessible treatment for patients using the blockchain network.

TMIS is a technology that enables physicians and patients to send and receive health services or medical information from remote sites. Hence, protecting the privacy of patient data is important. Table 6 presents a comprehensive analysis of previous studies on TMIS. Furthermore, Table 7 shows a comparison of the security properties of studies on TMIS. With the recent advance of blockchain technology, the IoT and telemedicine have increased. As a result, numerous studies investigated remote on-demand medical services provided by this technology [66–74]. The main objective of these studies is to overcome the distance obstacles and strengthen access to medical services in remote communities. The IoT phenomenon has provided an incredible service to a wide range of healthcare systems, allowing physicians to remotely diagnose patients. The studies that focus on the key challenges in the design of IoT-based RPM systems [56, 75–83]. These studies aggregate large data streams while ensuring patient confidentiality.

Table 6 also highlights the studies that utilise teledermatology inpatient care. These studies offer an opportunity to improve access to dermatological treatment through the use of telecommunications media to connect a variety of medical centres and exchange information on skin conditions over long distances [84]. Also, the telesurgery system has a tremendous potential to provide real-time surgical healthcare facilities over a wireless communication system to remote or distant areas with high quality and accuracy. The telesurgery system offers benefits to society by increasing accuracy and precision in surgical procedures [85]. Also, the current work evaluated these studies in terms of privacy and security to identify the impact of these studies in the aspects listed in Table 7.

5.2. E-health system

E-health is an innovation technology that has become critically important over time, ranging from remote access to patient-recorded medical data, such as EHR or electronic medical records (EMRs) to PHR from different on-site sensors to improve diagnosis. The capacity of blockchain is to store medical information over a decentralised storage

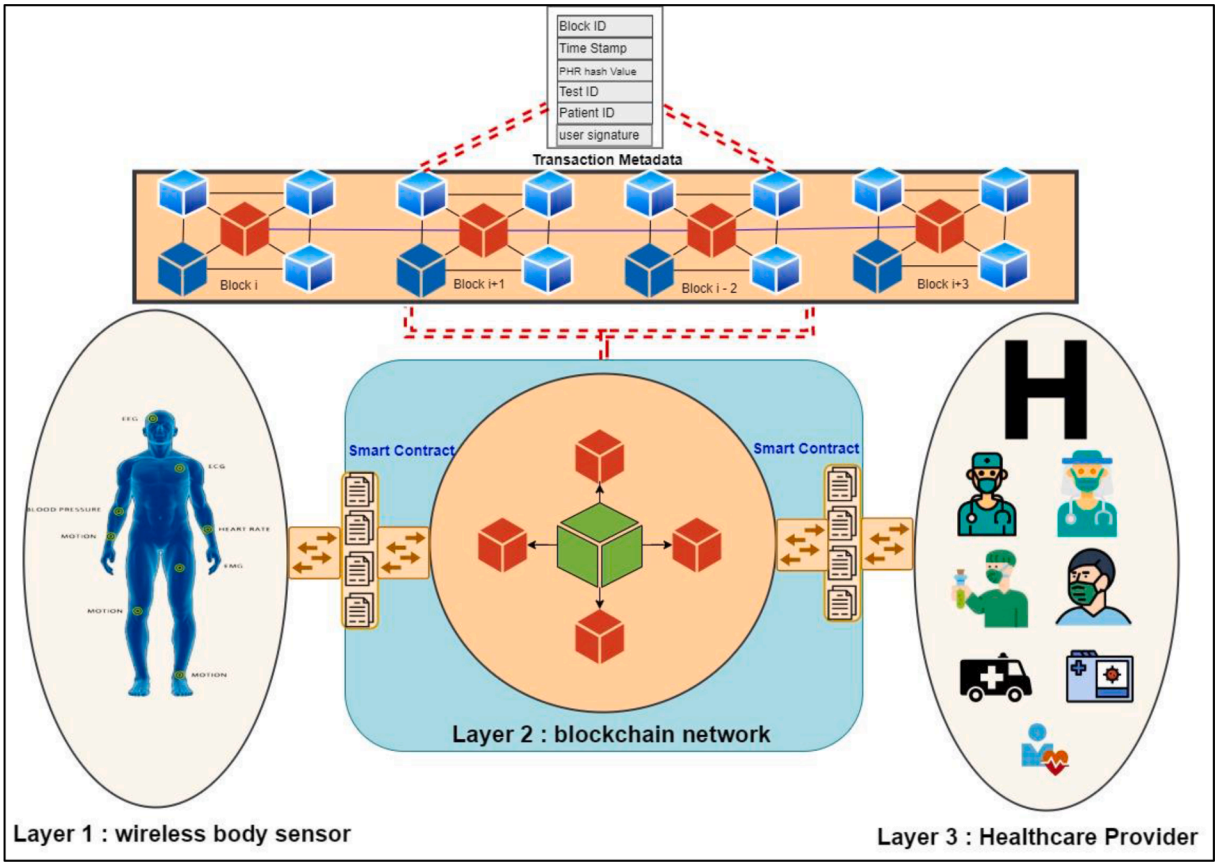

Fig. 14. General architecture of blockchain in *TIMS*.

Table 6
Comprehensive analysis of the literature on TMIS.

Ref.	Case study	Blockchain types	Problem addressed	Proposed solution	Major findings
[66]	Telemedicine system	Private blockchain	Cloud service provider and attribute-based encryption (ABE) of outsourcing healthcare data.	Multiple authorities ABE with update key policy and blockchain	Patients are allowed to register in a flexible manner and to change their access policies, while other unrelated patients are not required to renew their private registration keys and update their access policies.
[67]	Cancer therapy	Private blockchain	IoT sensor devices can be a single point of security failure, leading to the disruption of all network devices on the system.	Blockchain and off-chain storage framework	The conceptual system uses blockchain transactions to monitor a patient's physiological and mental state that can be shared with an oncologist or palliative care unit to securely and privately support real-time decision-making.
[68]	Smart healthcare	Consortium blockchain	Privacy-preserving and fine-grained access control of large-scale medical data in a blockchain	Blockchain and InterPlanetary File System (IPFS)	The IoT devices periodically send health information to the user node, then the user node encrypts the IoT data and sends it to the IPFS storage node.
[69]	Emergency medical services	Consortium blockchain (Hyperledger Fabric)	Patient's medical data history in an emergency situation.	Combination of blockchain, secured File transfer protocol and transport layer security	Enabling patient interaction and communication with multiple clinical and hospital departments in a secure manner by allowing only eligible users access to the data.
[70]	Smart hospital	Public blockchain	Centralised authentication mechanisms for the network of healthcare entities.	Blockchain and addition, rotation and XOR symmetric key encryption	Decentralised authentication of multiple entities in the hospital on the basis of blockchain by using ARX (SPECK) symmetric-key encryption to encrypt the blockchain data.
[71]	Medical smartphone networks	Consortium blockchain (Hyperledger Fabric)	The distributed nature of IoMT devices is insecure against insider attacks	Blockchain and Bayesian inference	Blockchain is used to improve Bayesian inference in trust management for detecting malicious nodes on medical smartphone networks.
[72]	EEG data	Private blockchain (Ethereum)	Malicious attacks, such as brain spyware, Btlejuice and replay, are capable of extracting user data, e.g. PIN, birthday and address, from user-recorded EEG signals.	Blockchain	Blockchain technology is capable of detecting changes in EEG data by employing the hash function based on the POW algorithm.
[73]	Finger vein biometrics	Private blockchain	The protection and confidentiality of data in the biometry of the finger vein	Combination of AES, blockchain and steganography techniques	Decentralised network architecture by employing blockchain and particle swarm optimisation steganography and advanced encryption standard AES for confidentiality in transmission channels.
[74]	Telemedicine system	Private blockchain (Ethereum)	The complexity and openness of data on the e-health care system against certain types of cyber attackers	Blockchain and order-preserving encryption scheme	MediBchain is proposed to leverage blockchain characteristics to realise a decentralised and privacy-preserving solution in TMIS. The double-anonymity scheme is used for anonymously authenticated patients and for monitoring malicious patients under necessary conditions. Certificateless authentication scheme ensures the confidentiality of the requested messages.
[75]	PSN-based healthcare	Private blockchain (Ethereum)	Overload computationally in sensor nodes	Blockchain and IEEE 802.15.6 authenticated protocol	The proposed method introduced protected links for PSN by using blockchain to exchange health data with others to improve the IEEE 802.15.6 authenticated association protocol version.
[76]	Remote diabetes monitoring	Private blockchain (Ethereum)	IoMT sensors and exchanging patient data between healthcare providers for diabetic diseases.	Blockchain and smart contracts	Leveraging blockchain and smart contracts features to keep all data secure and to track and formalise patient data in the event of an emergency.
[77]	Remote patient monitoring	Private blockchain	The mediator data processing centre in the RPM system causes security and fault tolerance bottlenecks within the protocol.	Blockchain, proximity user authentication (PUA) and keyed - hash message authentication code (HMAC)	Patient-centric agent system on the base of the blockchain is proposed. Secure authentication is achieved between BSN TO SDP by leveraging PUA and HMAC, and the confidentiality of health data is ensured by using AES-CTR encryption.
[78]	Remote patient monitoring	Private blockchain	Blockchain transaction and data storage restrictions	Blockchain and fuzzy inference process	The new architecture of the remote patient monitoring system is designed on the basis of blockchain technology to ensure the capacity of the body area sensor device. POW consensus mechanism is modified by using the fuzzy inference process to improve transaction performance.
[79]	Remote healthcare system	Private blockchain (Ethereum)	The security of streaming data in the IoT remote patient monitoring system	Blockchain and smart contracts	A remote healthcare system is proposed by using combined blockchain, smart contracts

(*continued on next page*)

Table 6 (*continued*)

Ref.	Case study	Blockchain types	Problem addressed	Proposed solution	Major findings
					and WBAN to protect the personal information and equipment and to notify the hospital if a patient is in danger.
[83]	Remote patient monitoring	Private blockchain (Ethereum)	Confidentiality and manageability of the transmission of health information	Blockchain and smart contracts	Remote patient monitoring is proposed using blockchain and smart contracts to perform real-time analysis and log transaction metadata for WBAN medical sensors.
[56]	Remote patient monitoring	Private blockchain (Ethereum)	Security concerns about the data transfer and the logging of data transactions and computational cost and high bandwidth	Blockchain, Off-chain storage, Tor network, and Ricochet with RSA algorithm,	Decentralised remote patient monitoring is proposed by using blockchain to eliminate a single point of failure or information. The PoA consensus mechanism used to ensure that the information is not altered for the transmitter and the recipient.
[80]	Wireless body area networks (WBANs)	Private blockchain	Unauthorised access of user data to the WBAN and modification of data stored in the system	Blockchain and sequential aggregate signature	Blockchain is used to prevent the data of WBAN users from being tampered with, and a sequential aggregate signature scheme is used to ensure that the information of the user can be viewed by the admin only.
[81]	WBANs	Private blockchain	Security of data sharing, computationally inefficient and high-energy consumption in WBANs	Blockchain, smart contracts, and attribute-based heterogeneous online/offline signcryption	The WBAN is proposed by using blockchain to comply with the security characteristics of non-repudiation and integrity of data sharing. Attribute-based signcryption for body sensor networks is used to ensure access data on the blockchain. It reduces the computational burden on biosensor nodes by using online/offline method.
[82]	WBANs	Consortium blockchain (Hyperledger Fabric)	The limited capacity of the traditional WBAN system due to the growing population of elderly people and chronic disease patients	Blockchain and IEEE 802.15.6 standard	The WBAN interoperable healthcare system is proposed based on blockchain in accordance with the specifications of IEEE 802.15.6. The system is compatible with low hardware utilisation while providing high-security protection and stable performance.
[84]	Teledermatology	Private blockchain (Ethereum)	The limitation of centralised teledermatology system in terms of interoperability	Blockchain	Teledermatology is proposed on the basis of the blockchain structure to ensure data maintenance and security of data sharing.
[85]	Telesurgery	Consortium blockchain (Hyperledger Fabric)	The limitation of the existing telesurgery system in terms of security, privacy and interoperability.	Blockchain and smart contracts.	The telesurgery framework is presented based on blockchain for secure and traceable patient treatment.
[86]	Telemedicine system	Consortium blockchain	The medical data stored on a cloud server in TMIS is a major target for an attacker due to its centralization system.	Blockchain, and ciphertext-policy attribute-based encryption (CP-ABE).	A secure authentication and access control protocols for a cloud-TMIS system are proposed using blockchain and CP-ABE to realize the integrity of medical data stored in cloud storage.
[87]	Telemedicine system	Consortium blockchain (Hyperledger Fabric)	A leak in the provision of an efficient and effective medical data preservation approach for TMIS.	Blockchain and elliptic curve cryptography.	Preservation medical data scheme for TMIS is proposed using blockchain and ECC-based Diffie-Hellman key exchange protocol in order to gain the features of tamper protection and decentralisation for data patients.
[88]	Internet of Medical Things (IoMT)	Private blockchain (Ethereum)	The limitation of the amalgamation of blockchain and smart contracts technologies into the IoMT application and balance between centralisation and decentralisation aspects.	Blockchain and smart contracts	The IoMT e-healthcare architecture is proposed with the use of a smart contracts and blockchain. The proposed architecture demonstrates that the smart contracts can handle the exchange of data on the heterogeneity of IoMT devices in a decentralised manner.
[89]	Remote patient monitoring	Consortium blockchain (Hyperledger Fabric)	The traditional RPM infrastructure system has drawback in aspects of the scalability and security	Blockchain, smart contracts and RESTful API	A novel remote patient monitoring system is proposed by using blockchain and smart contracts. The proposed system leverages the automated feature of the smart contracts to effectively read the vital signs of patients connecting to medical devices and exchange data with other authorised users on the network of blockchain.
[90]	Telemedicine system	Private blockchain (Ethereum)	Th current TMIS system unable to ensure the privacy and security aspects of exchange patient record with several medical professionals.	Blockchain, and Public key encryption with keyword search (PEKS)	Secure TMIS is introduced by combining blockchain and public key encryption with keyword search (PEKS) to guarantee confidentiality of patient records stored on third-party servers.

Table 7
Comparison of security properties of the literature on TMIS.

Ref.	Year	Access control	Authentication	Privacy protection	Integrity	Availability	Anonymity
[66]	2019	No	Yes	Yes	Yes	No	No
[67]	2019	Yes	No	No	Yes	No	No
[68]	2019	No	Yes	Yes	Yes	No	No
[69]	2020	Yes	No	No	Yes	No	No
[70]	2019	Yes	Yes	Yes	Yes	Yes	No
[71]	2019	Yes	No	No	Yes	No	No
[72]	2019	Yes	Yes	Yes	Yes	No	Yes
[73]	2018	Yes	No	No	Yes	No	No
[74]	2018	Yes	Yes	Yes	Yes	No	No
[75]	2016	Yes	No	No	Yes	No	No
[76]	2017	Yes	Yes	Yes	Yes	Yes	No
[77]	2018	Yes	No	No	Yes	No	Yes
[78]	2018	Yes	Yes	Yes	Yes	No	No
[79]	2019	Yes	No	No	Yes	No	No
[83]	2019	Yes	Yes	Yes	Yes	Yes	No
[56]	2018	No	No	Yes	Yes	No	No
[80]	2019	Yes	Yes	Yes	Yes	No	No
[81]	2019	Yes	No	No	Yes	No	Yes
[82]	2018	No	No	No	Yes	No	Yes
[84]	2019	Yes	No	No	Yes	No	Yes
[85]	2020	Yes	No	No	Yes	No	Yes
[86]	2020	Yes	Yes	No	Yes	No	No
[87]	2020	No	Yes	Yes	Yes	No	Yes
[88]	2020	No	No	No	Yes	No	Yes
[89]	2020	No	No	Yes	Yes	No	Yes
[90]	2020	No	Yes	Yes	Yes	No	No

that can only be accessed via smart contracts, as demonstrated in Fig. 15. Medical records can be portable and easy to transfer from one hospital to another to reduce additional costs of patients without repeat diagnostic tests. Also, it enables potential physicians to know the patient's medical history in an accessible manner so that patients can be treated accordingly. The transparency and manipulation of the patient's medical record is significantly achieved by storing every copy of the data on multiple nodes of the blockchain network [91–94]. Table 8 presents a comprehensive analysis of previous studies in the E-health system in terms of objective, case studies, major findings and security properties. Also, it demonstrates the evaluations of the security characteristics of the listed studies as follows: (1) user authentication, (2) authorisation or access control, (3) privacy preservation, (4) secure search (5) integrity, (6) availability and (7) anonymity.

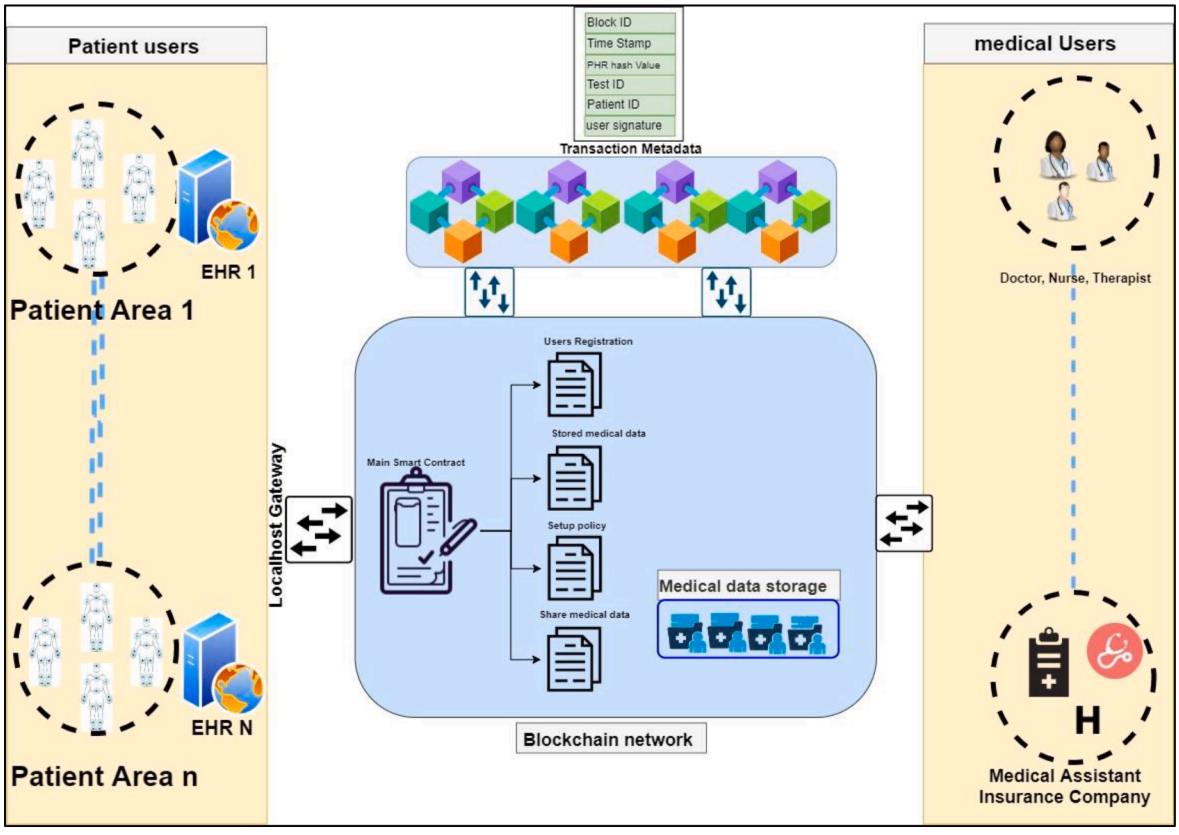

Fig. 15. General architecture of blockchain in *E-health*.

The sharing of EHR is of great importance for diagnosis and disease care to facilitate the treatment of patients by various medical professionals. In recent years, blockchain-based EHR sharing has made it easy to change the current network structure to a decentralised network to avoid imminent risks to data security and privacy [95,96,105,106, 97–104]. Blockchain plays a crucial role in the health information and sharing process by storing medical information in a secure form [107–111].

6. Discussion

The key elements of this emerging sector concentrate on motivations for the use of blockchain technology in the healthcare industry and open challenges that impede its usability. **Table 10** describes the motivation and challenges of adopting blockchain collaboration as a solution in the healthcare industry from a variety of perspectives. **Table 9** sheds light on the benefits and problems that have been addressed by blockchain use by healthcare industry entities.

6.1. Motivations

Blockchain technology is a product of modern society's effort to fulfil requirements in many applications of the healthcare industry. Blockchain technology can effectively enhance patient quality while preserving system security objectives. The various motivations and advantages of using blockchain technology in healthcare are explored, identified and grouped into categories extracted from a review of the studies to aid further discussion. **Fig. 16** demonstrates these motivation categories.

6.1.1. Decentralisation

The use of blockchain provides tremendous benefits for medical data by distributing it across the network rather than at a single central point to prevent a single point of security failure. This ecosystem allows for decentralised ownership of patient information, thus requiring all stakeholders in the healthcare industry to have seamless, secure and instant access to these data. This approach also allows the control of medical information to be transmitted and handled by an algorithm of consensus mechanism to be reached through shared feedback from the trusted entities in the network. The traditional healthcare industry network ecosystem has been turned into a decentralised network such as RPMs [75–78] teledermatology [84], telesurgery [85], EHRs [95,96], EMRs [108] and PHR systems [110,111]. This change has brought many benefits to the healthcare industry by solving a range of issues, such as patient records, the interoperability of the sharing of medical data and the protection of healthcare entities and medical care service.

6.1.2. Transparency

The transparency feature of blockchain utilises transactions and multilateral relationships that have been made more accurate, stable and efficient by the use of smart contracts. This feature addresses the lack of transparency in the healthcare industry for the admission of patients by providing strong potential for communication and dissemination of data amongst different healthcare providers. The patient transaction is automatically transferred to the doctor by means of a smart contracts, in which the patient communicates with the doctor before an appointment is issued. The transparency of data beyond the blockchain ensures trust between entities, which will contribute to the protection and tamper-proofness of medical data [104–106].

6.1.3. Security and privacy

The volume of medical data is growing, thus requiring creative processing and storage methods. Blockchain technology is used to illustrate the feasibility of protected healthcare storage and data transfer. Cryptography is used to protect nodes connected to a network in blockchain technology. The SHA-256 hash function algorithm is used to ensure that blockchains are secure by providing data integrity to prevent any manipulation. Cryptographic hashes are powerful functions that generate a digital data checksum that cannot extract any information from data stored in the blockchain without permission, thereby effectively protecting the privacy of health data [72,76,79,83–85].

6.2. Challenges

Blockchain offers several advantages in addressing the various issues of record sharing, security, and privacy with the healthcare industry. However, blockchain may not be the ideal solution that can be applied directly to the healthcare industry due to a number of drawbacks, such as scalability and storage capacity, blockchain size, standardisation and skill organisations. This section investigates and identifies the challenges posed by blockchain technology. **Fig. 17** shows the challenge categories.

6.2.1. Scalability and storage capacity issues

The storage of medical data on the blockchain causes two critical issues: confidentiality and scalability. The data on the blockchain are visible to everyone on the network because of the transparency and decentralised nature of the blockchain which is not suitable for certain applications in the healthcare industry. Data stored on the blockchain include patient medical history, laboratory tests, X-rays and MRI, which would have a major effect on the storage of the database [54].

6.2.2. Blockchain size issues

A sensor device connects to patients through blockchain transactions such as RPM [55] and EHRs [117], which would constantly increase the number of miners. Blockchain cannot handle a large amount of data streaming from IoMT devices [12,118,119].

6.2.3. Universal interoperability and standardisation issues

Blockchain is still in the early stages and is rapidly evolving, which is why no established standard for it is available yet. The implementation of blockchain technology in the healthcare sector would also take more time and effort for the organisation to adopt due to the need for international certified standardisation. The standard license would benefit from deciding on the size of the data, the data format and the type of data that could be stored on the blockchain. The adaptation of blockchain would become easier on the basis of defined standards, as they could easily be implemented in organisations [25,54].

6.2.4. Healthcare organisation skill issues

The concept of a blockchain technology business model is known to very few people. Completely switching the traditional RPM, EHR, PHR and EMR infrastructure to blockchain technology would be a time-consuming process for hospitals or any other healthcare organisation [27].

7. Prospects and future research directions

Blockchain technology has gained remarkable attention from many organisations and scholars in many areas and fields due to its capability to transform traditional industries with its features, such as suitability, decentralisation, persistence and anonymity [43]. Healthcare is one of the most important industries that can use this technology. In this research, many remarkable prospects and future directions were identified for scholars and organisations or industries.

7.1. Health data and sharing process

This investigation found that patient data can be truly owned and controlled by the patient. Furthermore, blockchain technology authorises health records to be time stamped, which means that no one can tamper with the records after they are stored in the distributed ledger. By employing blockchain technology, the patients have the right to

Table 8
Comprehensive analysis of the literature on an E-health system.

Reference	Case Study	Objective	1	2	3	4	5	6	7	Major Findings
[95]	EHR	To achieve multi-user data sharing of the blockchain EHR system through a proposed ABE.	×	√	×	√	√	×	×	The proposed EHR sharing scheme is based on the combination of permissioned blockchain and searchable ABE based on the assumption that patient privacy is not violated.
[96]	EHR	To present a new EHR system based on blockchain technology and ABE for secure and efficient recording and storing of medical data.	√	√	√	×	√	×	×	The proposed EHR scheme is incorporated with ABE and blockchain technology for efficient and scalable sharing of medical data and for protecting user privacy.
[97]	EHR	To design a new framework using cloud storage and keyless signature infrastructure that supports protect digital signatures, maintains security aspects and provides health records with integrity.	√	×	√	×	√	√	√	The proposed architecture guarantees the integrity and confidentiality of the data being managed in the EHR blockchain system by using the KSI digital signature.
[98]	EHR	To propose a private blockchain-based medical data exchange and security scheme to enhance patient mutual authentication and create a session key for their potential disease contact.	√	×	√	×	√	×	×	The proposed scheme is implemented on PBC and OpenSSL libraries in an EHR blockchain system.
[99]	EHR	To ensure confidentiality of outsourced EHRs from unauthorised modification without the involvement of any mediator.	√	×	√	×	√	×	×	The proposed scheme employs a user-friendly password-based key agreement to establish secure channels between patients and doctors in the EHR blockchain system.
[100]	EHR	To propose an authentication scheme for EHR based on blockchain.	√	×	√	×	√	×	×	The proposed scheme is assigned an identity-based signature (IBS) to ensure the authenticity of medical records in the consortium blockchain of the EHR system.
[101]	EHR	To ensure private medical data in the EHR cloud under the control of the only patient.	×	√	√	×	√	√	√	The proposed scheme implements elliptic curve cryptography along with blockchain technology to ensure the accountability, integrity, pseudonymity, security and privacy of medical records in the EHR system.
[102]	EHR	To propose a framework that can be used to incorporate blockchain technology in the EHR to address the issues of security, integrity and management of the EHR system.	×	×	√	×	√	×	×	The proposed scheme is implemented in a decentralised manner based on blockchain, which would store the patient's medical records and provide access to those records to solve problems aside from scalability by using off-chain scaling.
[103]	EHR	To remedy the challenging issue of reliably sharing EHRs amongst mobile users while maintaining high security in the mobile cloud.	×	√	×	×	√	√	×	The proposed scheme is combined with decentralised IPFS, cloud storage and blockchain technology to improve the protection of EHRs exchanging medical information in the EHR network while implementing a secure access control mechanism using smart contracts.
[104]	EHR	To present a method for locating relevant medical data on the EHR blockchain network and to acquire ciphertext re-encryption from the cloud server after the data owner has received authorisation.	×	√	√	√	√	√	×	The proposed architecture implements a cloud-aid blockchain that incorporates searchable encryption and proxy re-encryption techniques to achieve privacy and security of data sharing with EHR.
[105]	EHR	To enable physicians and researchers to obtain medical data of patients without revealing their personal details; this information should be exchanged amongst other qualified doctors.	×	√	√	√	√	×	×	The proposed architecture adopts a searchable encryption scheme for EHR-based blockchain to allow a third party to securely search for patient medical data.
[106]	EHR	To maintain authentication, integrity and confidentiality of health information by enabling fine-grained regulation of access in the EHR system.	√	√	√	×	√	√	×	The proposed platform adopts IBS and ABE for EHR-based blockchain to fulfil security and privacy requirements.
[91]	EHR	To design an EHR system based on technology of blockchain to enable the secure, reliable management, exchange, and aggregation of EHR data.	×	√	√	×	√	√	×	T he proposed system of EHR has allows patients to manage their medical records across several hospitals. At the same time, ensuring the privacy protection of patient data by setup an access control policy.
[92]	EHR	To enhance the privacy and data protection of the EHR system in the exchange of patient data across different healthcare services.	×	×	√	×	√	√	×	The proposed platform of blockchain EHR enable the data suppliers to interact with patients securely, quickly, easily and seamlessly.
[93]	EHR	To design and implement an EHR platform based on technology of blockchain for managing and tracking patient.	×	×	×	×	√	√	×	T he propsed platform leverages (IHE), (HL7) and (FHIR) standardisation to achieve interoperability in the implementation of the EHR blockchain.
[94]	EHR	To ensure confidentiality and integrity of the security factors for the sharing of sensitive health information between the different EHR systems	×	√	√	×	√	√	√	The proposed scheme combines Elliptic Curve Cryptography (ECC), Certificateless Aggregate Signature Scheme (CAS) and blockchain to secure the sharing and storage of EHR data in cloud storage.
[107]	EMR	To address data leakage in EMR that could lead to a privacy compromise.	×	×	√	×	√	×	×	The proposed EMR system architecture applies blockchain, proxy re-encryption and SHA-256 to

(*continued on next page*)

Table 8 (*continued*)

Reference	Case Study	Objective	1	2	3	4	5	6	7	Major Findings
										maintain interoperability, auditability and accessibility, security and access control, respectively.
[108]	EMR	To provide patients with accurate, immutable recording and ease of access to their medical records across healthcare services.	×	×	√	×	√	×	×	The proposed scheme deploys a medical blockchain network where personal medical data can be stored on an encrypted form and easily distributed amongst different healthcare players.
[112]	EMR	To propose a secure EMR scheme based on blockchain technology to protect the identity of the patient.	×	×	√	×	√	×	√	The proposed scheme integrates the attribute-based signature (ABS) with blockchain to insure that the user attributes are revoked and that the privacy of the patient's identity is protected.
[113]	EMR	To hide the sensitive data stored in mediator storage of the EMR system in way of maintaining the privacy of the patient.	×	×	√	×	√	×	×	The proposed architecture has established a lightweight privacy-preservation mechanism for blockchain EMRs by applying an techniques of interleaving encoder and (t, n) a threshold message sharing to encrypt the original patient data.
[114]	EMR	To proposed access control scheme for the EMR based on blockchain technology to enable patients to share their medical data securely.	×	√	√	×	√	×	×	The proposed access control scheme leverages the incentive mechanism of blockchain technology to aggressively exchange patient medical data in a feasible and practical manner.
[115]	EMR	To preserve the confidentiality of patients and secure the medical materials of the EMR system across the hospital.	√	√	√	×	√	√	×	The proposed EMR blockchain system is to exploit the internal function of smart contacts to support the authorization mechanism, mutual authentication to guarantee data integrity, non-repudiation, and traceability of users.
[109]	PHR	To ensure the sharing of personal medical data and reduce the cost of maintaining the data centre.	×	×	√	√	√	×	×	The proposed scheme was combined with blockchain technology, searchable symmetric encryption, and ABE techniques to secure the privacy of the PHR network.
[110]	PHR	To provide emergency access control management of patients for a PHR system.	×	√	√	×	√	×	×	The proposed implementation of a blockchain-based PHR network to address the needs of an emergency patient.
[111]	PHR	To address technical impediments beyond the use of blockchain in PHR systems, such as privacy issues, restricted storage and inefficient performance.	×	√	√	×	√	×	×	The proposed model uses blockchain technology and proxy re-encryption to support tamper resistance and preserve privacy, respectively.
[116]	PHR	To develop a platform for the exchange of medical information in the PHR system to ensure integrity, availability and confidentiality of patient records based on blockchain technology.	×	×	√	×	√	√	×	The proposed platform of PHR based on blockchain has an effective way to manage and share patient records with multiple health providers.

Table 9
Benefits of blockchain in the healthcare industry based on the current study.

Entities	Function	Solved problems
Patient	Patients are more easily able to view their own medical records. Deciding in which healthcare institution can patient data and medical records be obtained Diagnosis and treatment of patients in different hospitals or regions	No right to use patient data medical records without permission. Privacy issues Regional constraints
Hospital	Treatment of patients with less concern based on previous records	Current medical records are not reliable
Third-party healthcare institution	Blockchain platform is a more formal system for collecting comprehensive patient data.	Control of illegal access to patient data and medical records
Regulatory and auditing departments	Most patient treatments can be performed automatically by means of smart contracts.	High costs and low efficiency

authorise who can access their data. However, further studies are needed for numerous open challenges, such as health data cross-border sharing, which may hinder the advantages of blockchain data sharing. Moreover, individual privacy expectations differ between countries due to the regulation of each country's government. An urgent focus is needed on standardisations, regulations and retrieving policies of cross-border health data [101,107,108].

Table 10
Motivations and challenges.

Motivation	
Decentralisation	Medical data can be stored on the blockchain in a decentralised repository across the network.
Transparency	The medical data stored in blockchain repository are tamper-proof against manipulation.
Security and privacy	Blockchain is capable of ensuring the protection of medical data stored on it by using cryptographic algorithms.
Challenges	
Scalability, storage capacity	Inserting large volumes of medical data into the blockchain repository may cause storage and scalability issues.
Blockchain size	Blockchain is incapable of handling a large amount of data streaming from IoMT devices.
Universal interoperability and standardisation	Eliminating a previous healthcare system to a blockchain base is challenging due to its dramatic evolution, and it is a poorly understood technology by healthcare organisations.
Healthcare organisation skills	Implementing blockchain across a specific healthcare domain is difficult because no universally applicable established blockchain standards and principles exist.

7.2. Clinical trials

Clinical trials are performed to assess and evaluate the efficacy of any new drug that is developed and recommended for the treatment of a specific disease. New drugs can be tested on the basis of the success of the trial and can be utilised on a larger scale. Researchers conduct a clinical trial of drugs with a focus on various circumstances to generate

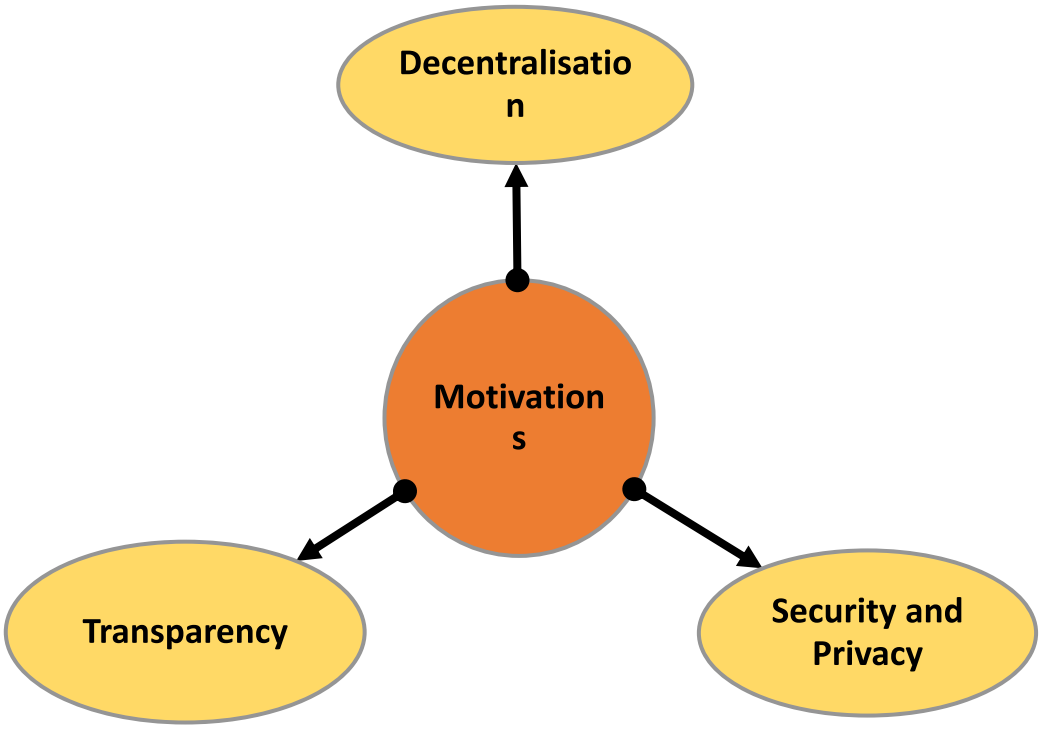

Fig. 16. Motivation for *blockchain use in the healthcare* industry.

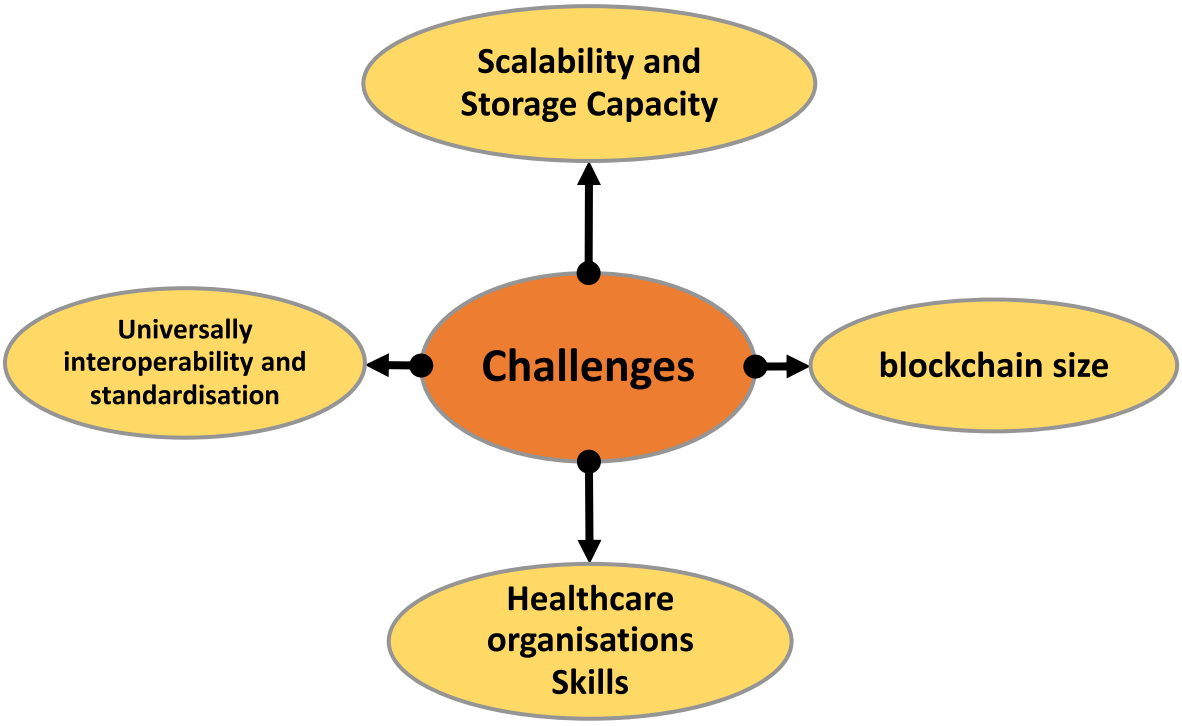

Fig. 17. Challenges faced by blockchain in the healthcare industry.

findings, statistical data and efficacy ratios for further drug decisions. Most of the pharmaceutical industry is willing to reveal the actual results of a drug analysis that can provide certain benefits for their businesses. However, some researchers often hide or modify their information and data collected to change the outcome. An appealing opportunity is the development of a decentralised blockchain-based system to ensure fair and transparent clinical trials and to improve data security. Three papers addressed the sharing of clinical data for use in non-clinical settings; two works designed an architecture called FHIRChain [120,121], and one developed a novel decentralised data management framework based on permissioned blockchain technology to reduce the administrative burden, time and effort of ensuring data integrity and privacy in multisite trials [122]. Blockchain needs to be used in clinical trials due to its success at large scales, and it could be a significant tool to identify an

effective vaccine for various types of diseases such as COVID-19, Ebola, SARS and MERS.

7.3. Pharmaceutical industry

Counterfeit medications can take the lives of thousands of people. The key feature of blockchain is utilised to ensure the traceability of medical products by providing a transparent decentralised tracking system. The immutability and timestamps of blockchain transactions can make it easy for drug manufacturers to track products and ensure that the information inside the block cannot be altered. This step can be performed by the data transparency feature in a blockchain to find the full path of counterfeit medication [123,124].

7.4. Real-time update and access of big data in the healthcare industry

Real-time updates and access features of big data in healthcare have a vital impact on the control and updating of patients' data [125,126]. The patient entity in a PHR system does not usually control their data stored in healthcare provider databases due to its centralised network. The integration of blockchain with PHRs has enabled patients to access and maintain their health history from a unified point of view on any device anywhere. Healthcare providers can access patient data stored in the blockchain and exchange data amongst health institutions [127]. The deployment of blockchain in PHRs is a substantial need due to its large-scale success and can be a practical tool for strengthening diagnosis accuracy and treatment effectiveness in the healthcare industry [128].

7.5. AI and 5 G ultrasonic device

Patient monitoring is valuable in conjunction with the development of an AI-enabled and 5 G ultrasonic system for emergency patients who require ultrasound. The development of remote control ultrasound based on 5 G wireless technology with intelligent navigation functions for capturing heart and lung views can provide an automatic measurement of key parameters and real-time guidance for ultrasound professionals and physicians. The adoption of blockchain technology is intended to improve the data storage of the WBAN to improve the protection of collected data. A decentralised architecture system needs to be proposed for transferring patient data from one affiliated hospital to another without re-authentication requirements, resulting in reduced overall delay in the exchange of information across the network [66–74]

7.6. Intelligent monitoring system and high-throughput screening technology

The whole world has been attacked by COVID-19, which has resulted in a very serious situation today. The development of an intelligent monitoring system on a wearable monitoring device in quarantine installations and a high-performance screening system for the identification of virus carriers in high-flow-density public places is essential. The system uses a body temperature sensor to collect data from patients on the forehead or underarm, and data are then sent to a cloud server to notify the healthcare provider of high body temperatures. The reliability of trust management on intelligent monitoring system medical smartphone networks must be investigated by leveraging the advantages of blockchain technology such as trustworthiness, immutability and integrity in WSNs [71–73].

7.7. Security and privacy

The exchange of patient data amongst different healthcare providers helps prevent medication errors and enhances the quality of patient diagnostic treatment. Concerns about security and privacy are amongst the main reasons providers are unwilling to share data.

7.7.1. User authentication

Healthcare players are exposed to many security issues such as user authentication attack and replay attacks. Hospital authorities are responsible for ensuring that patient data are authenticated and for monitoring the maintenance of protected patient records. No work considers the issue of authentication users for blockchain development on EHRs, PHRs and EMRs, where the scheme suffers from collusion attack problems and an incompatible blockchain model. An essential detail to consider is the authentication enrolment of users in a system of multiple healthcare entities, such as hospitals, medical insurance providers, scientific research institutions, and pharmaceutical companies, which is more suitable for real-world applications.

7.7.2. Authorisation and access control

Blockchain provides potential solutions for the healthcare industry due to its irreversibility and immutability. The transparency of blockchain enables all healthcare players in the network to view all the data that lead to confidentiality issues. A model that includes fine-grained and efficient access control for healthcare players needs to be proposed to address this blockchain drawback through the utilisation of cryptographic primitives such as ABE algorithm.

7.7.3. Secure search

The blockchain solution for EHRs, PHRs and EMRs is a feasible approach that enables one to develop a system on cryptographic algorithms to ensure data integrity. A searchable mechanism for the healthcare system is important in the sharing of real data to ensure that medical data can be accessed only by authorised entities. A prospective research direction is to propose a searchable framework for a blockchain healthcare player system on the basis of searchable encryption, in which only the query index is attached to the public blockchain to enable the dissemination of medical data, while the actual medical data are stored in encrypted form on a cloud server. This concept demonstrates the potential of using an algorithm to support a sophisticated query that enables multiple healthcare providers to gain authorisation to access health records and to communicate with one another.

8. Conclusion

The limitations of this work are the databases employed in our search. Moreover, blockchain activities in the healthcare industries have increased, thereby affecting the timeline of the study. However, the objective of this study is to identify the gap in blockchain and the healthcare industries by assessing the broad blockchain research conducted on the healthcare industries so far. Numerous scholars have examined blockchain technology in the healthcare industries. In this research, bibliometric analysis was conducted on the blockchain and healthcare studies. This study has a significant impact on the development of the healthcare industry. The following concluding statements are constructed:

- This work presents several universal research phases of blockchain and healthcare industry activities conducted by scholars and organisations. The analysis of data distribution, keywords, research area, venues and citations indicated that scholars use blockchain to resolve difficulties in the healthcare industry.
- Case studies of blockchain use in healthcare, such as TMIS and E-health system, were conducted.
- This study discussed the motivation for scholars and researchers and highlighted the challenges that can be faced in the study of blockchain in the healthcare industries.
- Research prospects are available for researchers and organisations in many aspects, such as the health data sharing process, clinical trials, the pharmaceutical industry, updating and access of big data, AI, 5 G ultrasonic device, security and privacy.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

The authors are grateful to Universiti Putra Malaysia for their generous support.

References

[1] M.A. Khan, K. Salah, IoT security: review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. 82 (2018) 395–411.
[2] T.M. Fernández-Caramés, P. Fraga-Lamas, A Review on the Use of Blockchain for the Internet of Things, Ieee Access 6 (2018) 32979–33001.
[3] M.C.K. Khalilov, A. Levi, A survey on anonymity and privacy in bitcoin-like digital cash systems, IEEE Commun. Surv. Tutorials 20 (3) (2018) 2543–2585.
[4] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Gener. Comput. Syst. 107 (2020) 841–853.
[5] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where is current research on blockchain technology?—A systematic review, PLoS ONE 11 (10) (2016), e0163477.
[6] A. Khatoon, A blockchain-based smart contract system for healthcare management, Electronics (Basel) 9 (1) (2020) 94.
[7] Y. Lu, Blockchain: a survey on functions, applications and open issues, J. Ind.l Integr. Manag. 3 (04) (2018), 1850015.
[8] Y. Lu, Blockchain and the related issues: a review of current research topics, J. Manag. Anal. 5 (4) (2018) 231–255.
[9] S. Perera, S. Nanayakkara, M.N.N. Rodrigo, S. Senaratne, R. Weinand, Blockchain technology: is it hype or real in the construction industry? J. Indus. Inf. Integr. 17 (2020), 100125.
[10] W. Viriyasitavat, D. Hoonsopon, Blockchain characteristics and consensus in modern business processes, J. Indus. Inf. Integr. 13 (2019) 32–39.
[11] Y. Lu, The blockchain: state-of-the-art and research challenges, J. Indus. Inf. Integr. 15 (2019) 80–90.
[12] W. Viriyasitavat, T. Anuphaptrirong, D. Hoonsopon, When blockchain meets internet of things: characteristics, challenges, and business opportunities, J. Indus. Inf. Integr. 15 (2019) 21–28.
[13] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, Fog computing for Healthcare 4.0 environment: opportunities and challenges, Computers & Electrical Engineering 72 (2018) 1–13.
[14] A. Gorkhali, L. Li, A. Shrestha, Blockchain: a literature review, J. Manag. Anal. 7 (3) (2020) 321–343.
[15] S. Demirkan, I. Demirkan, A. McKee, Blockchain technology in the future of business cyber security and accounting, J. Manag. Anal. 7 (2) (2020) 189–208.
[16] H. Hassani, X. Huang, E. Silva, Banking with blockchain-ed big data, J. Manag. Anal. 5 (4) (2018) 256–275.
[17] S. Tanwar, K. Parekh, R. Evans, Blockchain-based electronic healthcare record system for healthcare 4.0 applications, J. Inf. Secur. Appl. 50 (2020), 102407.
[18] L. Ismail, H. Materwala, S. Zeadally, Lightweight blockchain for healthcare, IEEE Access 7 (2019) 149935–149951.
[19] Z. Shae, J.J. Tsai, On the design of a blockchain platform for clinical trial and precision medicine, in: 2017 IEEE 37th international conference on distributed computing systems (ICDCS), IEEE, 2017, pp. 1972–1980.
[20] C. Mandolla, A.M. Petruzzelli, G. Percoco, A. Urbinati, Building a digital twin for additive manufacturing through the exploitation of blockchain: a case analysis of the aircraft industry, Comput. Ind. 109 (2019) 134–152.
[21] G. Zhao, S. Liu, C. Lopez, H. Lu, S. Elgueta, H. Chen, B.M. Boshkoska, Blockchain technology in agri-food value chain management: a synthesis of applications, challenges and future research directions, Comput. Ind. 109 (2019) 83–99.
[22] E. Hofmann, M. Rüsch, Industry 4.0 and the current status as well as future prospects on logistics, Comput. Ind. 89 (2017) 23–34.
[23] M. Hölbl, M. Kompara, A. Kamišalić, L. Nemec Zlatolas, A systematic review of the use of blockchain in healthcare, Symmetry (Basel) 10 (10) (2018) 470.
[24] G.J. Katuwal, S. Pandey, M. Hennessey, B. Lamichhane, Applications of Blockchain in Healthcare: Current Landscape & Challenges, 2018 *arXiv preprint arXiv:1812.02776*.
[25] A.A. Siyal, A.Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, G. Soursou, Applications of blockchain technology in medicine and healthcare: challenges and future perspectives, Cryptography 3 (1) (2019) 3.
[26] Boulos, M.N.K., Wilson, J.T. and Clauson, K.A., 2018. Geospatial blockchain: promises, challenges, and scenarios in health and healthcare.
[27] S.G. Alonso, J. Arambarri, M. López-Coronado, I. de la Torre Díez, Proposing new blockchain challenges in ehealth, J. Med Syst 43 (3) (2019) 64.
[28] T. McGhin, K.K.R. Choo, C.Z. Liu, D. He, Blockchain in healthcare applications: research challenges and opportunities, J. Netw. Comput. Appl. 135 (2019) 62–75.
[29] C.C. Agbo, Q.H. Mahmoud, J.M. Eklund, Blockchain technology in healthcare: a systematic review, Healthcare 7 (2) (2019) 56.
[30] S. Khezr, M. Moniruzzaman, A. Yassine, R. Benlamri, Blockchain technology in healthcare: a comprehensive review and directions for future research, Appl. Sci. 9 (9) (2019) 1736.
[31] M. Hölbl, M. Kompara, A. Kamišalić, L. Nemec Zlatolas, A systematic review of the use of blockchain in healthcare, Symmetry (Basel) 10 (10) (2018) 470.
[32] M. Aria, C. Cuccurullo, bibliometrix: an R-tool for comprehensive science mapping analysis, J. Informetr. 11 (4) (2017) 959–975.
[33] M. Dabbagh, M. Kakavand, M. Tahir, Towards Integration of Blockchain and IoT: a Bibliometric Analysis of State-of-the-Art, in: International Congress on Blockchain and Applications, Springer, Cham, 2019, pp. 27–35.
[34] M. Dabbagh, M. Sookhak, N.S. Safa, The evolution of blockchain: abibliometric study, Ieee Access 7 (2019) 19212–19221.
[35] H.M. Rouzbahani, H. Karimipour, A. Dehghantanha, R.M. Parizi, Blockchain applications in power systems: a bibliometric analysis. Blockchain Cybersecurity, Trust and Privacy, Springer, Cham, 2020, pp. 129–145.
[36] S. Zeng, X. Ni, Y. Yuan, F.Y. Wang, A bibliometric analysis of blockchain research, in: 2018 IEEE intelligent vehicles symposium (IV), IEEE, 2018, pp. 102–107.
[37] I. Merediz-Solà, A.F. Bariviera, A bibliometric analysis of bitcoin scientific production, Res. Int. Bus. Financ. 50 (2019) 294–305.
[38] M. Kamran, H.U. Khan, W. Nisar, M. Farooq, S.U. Rehman, Blockchain and internet of things: a bibliometric study, Comput. Electr. Eng. 81 (2020), 106525.
[39] H.H. Altarturi, M. Saadoon, N.B. Anuar, Cyber parental control: a bibliometric study, Child Youth Serv. Rev. (2020), 105134.
[40] W. Viriyasitavat, L. Da Xu, Z. Bi, A. Sapsomboon, Blockchain-based business process management (BPM) framework for service composition in industry 4.0, J. Intell. Manuf. (2018) 1–12.
[41] W. Viriyasitavat, L. Da Xu, Z. Bi, D. Hoonsopon, Blockchain technology for applications in internet of things—mapping from system design perspective, IEEE Int. Things J. 6 (5) (2019) 8155–8168.
[42] L. Da Xu, W. Viriyasitavat, Application of blockchain in collaborative Internet-of-Things services, IEEE Trans. Comput. Soc. Syst. 6 (6) (2019) 1295–1305.
[43] W. Viriyasitavat, L. Da Xu, Z. Bi, V. Pungpapong, Blockchain and internet of things for modern business process in digital economy—the state of the art, IEEE Trans. Comput. Soc. Syst. 6 (6) (2019) 1420–1432.
[44] L.D. Xu, E.L. Xu, L. Li, Industry 4.0: state of the art and future trends, Int. J. Prod. Res. 56 (8) (2018) 2941–2962.
[45] C. Zhang, Y. Chen, A review of research relevant to the emerging industry trends: industry 4.0, IoT, blockchain, and business analytics, J. Ind.l Integr. Manag. 5 (01) (2020) 165–180.
[46] P. Zhang, D.C. Schmidt, J. White, A. Dubey, Consensus mechanisms and information security technologies, in: Advances in Computers, 115, Elsevier, 2019, pp. 181–209.
[47] W. Wang, D.T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, D.I. Kim, A survey on consensus mechanisms and mining strategy management in blockchain networks, IEEE Access 7 (2019) 22328–22370.
[48] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J.A. Kroll, E.W. Felten, Sok: research perspectives and challenges for bitcoin and cryptocurrencies, in: 2015 IEEE Symposium on Security and Privacy, IEEE, 2015, pp. 104–121.
[49] P. Pandey, R. Litoriya, Implementing healthcare services on a large scale: challenges and remedies based on blockchain technology, Health Policy Technol. 9 (1) (2020) 69–78.
[50] A. Li, X. Wei, Z. He, Robust proof of stake: a new consensus protocol for sustainable blockchain systems, Sustainability 12 (7) (2020) 2824.
[51] M. Castro, B. Liskov, Practical Byzantine fault tolerance, OSDI 99 (1999) (1999) 173–186.
[52] I.M. Coelho, V.N. Coelho, R.P. Araujo, W.Y. Qiang, B.D. Rhodes, Challenges of PBFT-inspired consensus for blockchain and enhancements over Neo dBFT, Future Internet 12 (8) (2020) 129.
[53] A. Hasselgren, K. Kralevska, D. Gligoroski, S.A. Pedersen, A. Faxvaag, Blockchain in healthcare and health sciences—a scoping review, Int. J. Med Inform 134 (2020), 104040.
[54] H.M. Hussien, S.M. Yasin, S.N.I. Udzir, A.A. Zaidan, B.B. Zaidan, A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction, J. Med. Syst. 43 (10) (2019) 320.
[55] K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, J. Med. Syst. 42 (7) (2018) 130.
[56] M.S. Ali, M. Vecchio, G.D. Putra, S.S. Kanhere, F. Antonelli, A decentralized peer-to-peer remote health monitoring system, Sensors 20 (6) (2020) 1656.
[57] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control, J. Med. Syst. 40 (10) (2016) 218.
[58] Q.I. Xia, E.B. Sifah, K.O. Asamoah, J. Gao, X. Du, M. Guizani, MeDShare: trust-less medical data sharing among cloud service providers via blockchain, IEEE Access 5 (2017) 14757–14767.
[59] J. Zhang, N. Xue, X. Huang, A secure system for pervasive social network-based healthcare, Ieee Access 4 (2016) 9239–9250.
[60] X. Liang, J. Zhao, S. Shetty, J. Liu, D. Li, Integrating blockchain for data sharing and collaboration in mobile healthcare applications, in: 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), IEEE, 2017, pp. 1–5.
[61] R. Guo, H. Shi, Q. Zhao, D. Zheng, Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems, IEEE Access 6 (2018) 11676–11686.

[62] A. Roehrs, C.A. da Costa, R. da Rosa Righi, OmniPHR: a distributed architecture model to integrate personal health records, J. Biomed. Inform. 71 (2017) 70–81.
[63] A.D. Dwivedi, G. Srivastava, S. Dhar, R. Singh, A decentralized privacy-preserving healthcare blockchain for IoT, Sensors 19 (2) (2019) 326.
[64] K. Fan, S. Wang, Y. Ren, H. Li, Y. Yang, Medblock: efficient and secure medical data sharing via blockchain, J. Med. Syst. 42 (8) (2018) 136.
[65] A. Zhang, X. Lin, Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain, J. Med. Syst. 42 (8) (2018) 140.
[66] R. Guo, H. Shi, D. Zheng, C. Jing, C. Zhuang, Z. Wang, Flexible and efficient blockchain-based ABE scheme with multi-authority for medical on demand in telemedicine system, IEEE Access 7 (2019) 88012–88025.
[67] M.A. Rahman, M. Rashid, S. Barnes, M.S. Hossain, E. Hassanain, M. Guizani, An IoT and blockchain-based multi-sensory in-home quality of life framework for cancer patients, in: 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), IEEE, 2019, pp. 2116–2121.
[68] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, N. Yu, Healthchain: a blockchain-based privacy preserving scheme for large-scale health data, IEEE Int. Things J. 6 (5) (2019) 8770–8781.
[69] S. Hasavari, Y.T. Song, A secure and scalable data source for emergency medical care using blockchain technology, in: 2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA), IEEE, 2019, pp. 71–75.
[70] A. Yazdinejad, G. Srivastava, R.M. Parizi, A. Dehghantanha, K.K.R. Choo, M. Aledhari, Decentralized authentication of distributed patients in hospital networks using blockchain, in: IEEE Journal of Biomedical and Health Informatics, 2020.
[71] W. Meng, W. Li, L. Zhu, Enhancing medical smartphone networks via blockchain-based trust management against insider attacks, in: IEEE Transactions on Engineering Management, 2019.
[72] S. Bak, Y. Pyo, J. Jeong, Protection of EEG data using blockchain platform, in: 2019 7th International Winter Conference on Brain-Computer Interface (BCI), IEEE, 2019, pp. 1–3.
[73] A.H. Mohsin, A.A. Zaidan, B.B. Zaidan, O.S. Albahri, A.S. Albahri, M.A. Alsalem, K.I. Mohammed, Based blockchain-PSO-AES techniques in finger vein biometrics: a novel verification secure framework for patient authentication, Comput. Standards Interf. 66 (2019), 103343.
[74] Y. Ji, J. Zhang, J. Ma, C. Yang, X. Yao, BMPLS: blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems, J. Med. Syst. 42 (8) (2018) 147.
[75] J. Zhang, N. Xue, X. Huang, A secure system for pervasive social network-based healthcare, Ieee Access 4 (2016) 9239–9250.
[76] M. Saravanan, R. Shubha, A.M. Marks, V. Iyer, SMEAD: a secured mobile enabled assisting device for diabetics monitoring, in: 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), IEEE, 2017, pp. 1–6.
[77] M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, Continuous patient monitoring with a patient centric agent: a block architecture, IEEE Access 6 (2018) 32700–32726.
[78] M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, A decentralized patient agent controlled blockchain for remote patient monitoring, in: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2019, pp. 1–8.
[79] H.L. Pham, T.H. Tran, Y. Nakashima, A secure remote healthcare system for hospital using blockchain smart contract, in: 2018 IEEE Globecom Workshops (GC Wkshps), IEEE, 2018, pp. 1–6.
[80] Y. Ren, Y. Leng, F. Zhu, J. Wang, H.J. Kim, Data storage mechanism based on blockchain with privacy protection in wireless body area network, Sensors 19 (10) (2019) 2395.
[81] J. Iqbal, A.I. Umar, N. Amin, A. Waheed, Efficient and secure attribute-based heterogeneous online/offline signcryption for body sensor networks based on blockchain, Int. J. Distrib. Sens. Netw. 15 (9) (2019), 1550147719875654.
[82] J. Wang, K. Han, A. Alexandridis, Z. Chen, Z. Zilic, Y. Pang, G. Jeon, F. Piccialli, A blockchain-based eHealthcare system interoperating with WBANs, Future Gener. Comput. Syst. 110 (2020) 675–685.
[83] K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, J. Med. Syst. 42 (7) (2018) 130.
[84] K. Mannaro, G. Baralla, A. Pinna, S. Ibba, A blockchain approach applied to a teledermatology platform in the Sardinian region (Italy), Information 9 (2) (2018) 44.
[85] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M.S. Obaidat, B. Sadoun, HaBiTs: blockchain-based telesurgery framework for healthcare 4.0, in: 2019 International Conference on Computer, Information and Telecommunication Systems (CITS), IEEE, 2019, pp. 1–5.
[86] S. Son, J. Lee, M. Kim, S. Yu, A.K. Das, Y. Park, Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain, IEEE Access 8 (2020) 192177–192191.
[87] T.F. Lee, H.Z. Li, Y.P. Hsieh, A blockchain-based medical data preservation scheme for telecare medical information systems, Int. J. Inf. Secur. (2020) 1–13.
[88] A. Sharma, R. Tomar, N. Chilamkurti, B.G. Kim, Blockchain based smart contracts for internet of medical things in e-healthcare, Electronics (Basel) 9 (10) (2020) 1609.
[89] F. Jamil, S. Ahmad, N. Iqbal, D.H. Kim, Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals, Sensors 20 (8) (2020) 2195.
[90] S. Shamshad, K. Mahmood, S. Kumari, C.M. Chen, A secure blockchain-based e-health records storage and sharing scheme, J. Inf. Secur. Appl. 55 (2020), 102590.
[91] S. Niu, L. Chen, J. Wang, F. Yu, Electronic health record sharing scheme with searchable attribute-based encryption on blockchain, IEEE Access 8 (2019) 7195–7204.
[92] S.M. Pournaghi, M. Bayat, Y. Farjami, MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption, J Ambient. Intell. Humaniz. Comput. (2020) 1–29.
[93] L. Chen, W.K. Lee, C.C. Chang, K.K.R. Choo, N. Zhang, Blockchain based searchable encryption for electronic health record sharing, Future Gener. Comput. Syst. 95 (2019) 420–429.
[94] H. Wang, Y. Song, Secure cloud-based EHR system using attribute-based cryptosystem and blockchain, J. Med. Syst. 42 (8) (2018) 152.
[95] G. Nagasubramanian, R.K. Sakthivel, R. Patan, A.H. Gandomi, M. Sankayya, B. Balusamy, Securing e-health records using keyless signature infrastructure blockchain technology in the cloud, Neural Comput. Appl. 32 (3) (2020) 639–647.
[96] X. Liu, Z. Wang, C. Jin, F. Li, G. Li, A blockchain-based medical data sharing and protection scheme, IEEE Access 7 (2019) 118943–118953.
[97] S. Cao, G. Zhang, P. Liu, X. Zhang, F. Neri, Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain, Inf. Sci. (Ny) 485 (2019) 427–440.
[98] F. Tang, S. Ma, Y. Xiang, C. Lin, An efficient authentication scheme for blockchain-based electronic health records, IEEE access 7 (2019) 41678–41689.
[99] A. Al Omar, M.Z.A. Bhuiyan, A. Basu, S. Kiyomoto, M.S. Rahman, Privacy-friendly platform for healthcare data in cloud based on blockchain environment, Future Gener. Comput. Syst. 95 (2019) 511–521.
[100] A. Shahnaz, U. Qamar, A. Khalid, Using blockchain for electronic health records, IEEE Access 7 (2019) 147782–147795.
[101] D.C. Nguyen, P.N. Pathirana, M. Ding, A. Seneviratne, Blockchain for secure ehrs sharing of mobile cloud based e-health systems, IEEE Access 7 (2019) 66792–66806.
[102] Y. Wang, A. Zhang, P. Zhang, H. Wang, Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain, IEEE Access 7 (2019) 136704–136719.
[103] E.Y. Daraghmi, Y.A. Daraghmi, S.M. Yuan, MedChain: a design of blockchain-based system for medical records access and permissions management, IEEE Access 7 (2019) 164595–164613.
[104] L. Hang, E. Choi, D.H. Kim, A novel EMR integrity management based on a medical blockchain platform in hospital, Electronics (Basel) 8 (4) (2019) 467.
[105] S. Wang, D. Zhang, Y. Zhang, Blockchain-based personal health records sharing scheme with data integrity verifiable, IEEE Access 7 (2019) 102887–102901.
[106] A.R. Rajput, Q. Li, M.T. Ahvanooey, I. Masood, EACMS: emergency access control management system for personal health record based on blockchain, IEEE Access 7 (2019) 84304–84317.
[107] T.T. Thwin, S. Vasupongayya, Blockchain-based access control model to preserve privacy for personal health record systems, in: Security and Communication Networks 2019, 2019.
[108] A. Dubovitskaya, F. Baig, Z. Xu, R. Shukla, P.S. Zambani, A. Swaminathan, M. M. Jahangir, K. Chowdhry, R. Lachhani, N. Idnani, M. Schumacher, ACTION-EHR: patient-centric blockchain-based electronic health record data management for cancer care, J. Med. Internet Res. 22 (8) (2020) e13598.
[109] H. Liu, R.G. Crespo, O.S. Martínez, Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts, Healthcare 8 (3) (2020) 243.
[110] A. Margheri, M. Masi, A. Miladi, V. Sassone, J. Rosenzweig, Decentralised provenance for healthcare data, Int. J. Med. Inform. (2020), 104197.
[111] T. Benil, J. Jasper, Cloud based security on outsourcing using blockchain in E-health systems, Comput. Networks (2020), 107344.
[112] Q. Su, R. Zhang, R. Xue, P. Li, Revocable attribute-based signature for blockchain-based healthcare system, IEEE Access 8 (2020) 127884–127896.
[113] J. Fu, N. Wang, Y. Cai, Privacy-preserving in healthcare blockchain systems based on lightweight message sharing, Sensors 20 (7) (2020) 1898.
[114] C. Gan, A. Saini, Q. Zhu, Y. Xiang, Z. Zhang, Blockchain-based access control scheme with incentive mechanism for eHealth systems: patient as supervisor, Multimed. Tools Appl. (2020) 1–17.
[115] C.L. Chen, Y.Y. Deng, W. Weng, H. Sun, M. Zhou, A blockchain-based secure inter-hospital EMR sharing system, Appl. Sci. 10 (14) (2020) 4958.
[116] H.A. Lee, H.H. Kung, J.G. Udayasankaran, B. Kijsanayotin, A.B. Marcelo, L. R. Chao, C.Y. Hsu, An architecture and management platform for blockchain-based personal health record exchange: development and usability study, J. Med. Internet Res. 22 (6) (2020) e16748.
[117] S. Badr, I. Gomaa, E. Abd-Elrahman, Multi-tier blockchain framework for IoT-EHRs systems, Procedia Comput. Sci. 141 (2018) 159–166.
[118] W. Viriyasitavat, L. Da Xu, Z. Bi, A. Sapsomboon, New blockchain-based architecture for service interoperations in internet of things, IEEE Trans. Comput. Soc. Syst. 6 (4) (2019) 739–748.
[119] W. Viriyasitavat, L. Da Xu, Z. Bi, D. Hoonsopon, N. Charoenruk, Managing qos of internet-of-things services using blockchain, IEEE Trans. Comput. Soc. Syst. 6 (6) (2019) 1357–1368.
[120] P. Zhang, J. White, D.C. Schmidt, G. Lenz, S.T. Rosenbloom, FHIRChain: applying blockchain to securely and scalably share clinical data, Comput. Struct. Biotechnol. J. 16 (2018) 267–278.
[121] I. Kotsiuba, A. Velvkzhanin, Y. Yanovich, I.S. Bandurova, Y. Dyachenko, V. Zhygulin, Decentralized e-Health architecture for boosting healthcare

analytics, in: 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), IEEE, 2018, pp. 113–118.
[122] O. Choudhury, N. Fairoza, I. Sylla, A. Das, A Blockchain Framework For Managing and Monitoring Data in Multi-Site Clinical Trials, 2019 *arXiv preprint arXiv: 1902.03975*.
[123] P. Pandey, R. Litoriya, Securing E-health networks from counterfeit medicine penetration using Blockchain, Wireless Personal Commun. (2020) 1–19.
[124] H. Kaur, M.A. Alam, R. Jameel, A.K. Mourya, V. Chang, A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment, J. Med. Syst. 42 (8) (2018) 156.
[125] G. Aceto, V. Persico, A. Pescapé, Industry 4.0 and health: internet of things, big data, and cloud computing for healthcare 4.0, J. Indus. Inf. Integr. 18 (2020), 100129.
[126] I.C. Reinhardt, J.C. Oliveira, D.T. Ring, Current perspectives on the development of Industry 4.0 in the pharmaceutical sector, J. Indus. Inf. Integr. 18 (2020), 100131.
[127] E.J. De Aguiar, B.S. Faiçal, B. Krishnamachari, J. Ueyama, A survey of blockchain-based strategies for healthcare, ACM Comput. Surv. (CSUR) 53 (2) (2020) 1–27.
[128] S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, F.Y. Wang, Blockchain-powered parallel healthcare systems based on the ACP approach, IEEE Trans. Comput. Soc. Syst. 5 (4) (2018) 942–950.